CYBERSECURITY OF VOTING MACHINES

JOINT HEARING

BEFORE THE

SUBCOMMITTEE ON
INFORMATION TECHNOLOGY

AND THE

SUBCOMMITTEE ON
INTERGOVERNMENTAL AFFAIRS

OF THE

COMMITTEE ON OVERSIGHT
AND GOVERNMENT REFORM
HOUSE OF REPRESENTATIVES

ONE HUNDRED FIFTEENTH CONGRESS

FIRST SESSION

NOVEMBER 29, 2017

Serial No. 115–64

Printed for the use of the Committee on Oversight and Government Reform

Available via the World Wide Web: http://www.fdsys.gov
http://oversight.house.gov

U.S. GOVERNMENT PUBLISHING OFFICE
30–295 PDF WASHINGTON : 2018

Committee on Oversight and Government Reform

Trey Gowdy, South Carolina, *Chairman*

John J. Duncan, Jr., Tennessee
Darrell E. Issa, California
Jim Jordan, Ohio
Mark Sanford, South Carolina
Justin Amash, Michigan
Paul A. Gosar, Arizona
Scott DesJarlais, Tennessee
Blake Farenthold, Texas
Virginia Foxx, North Carolina
Thomas Massie, Kentucky
Mark Meadows, North Carolina
Ron DeSantis, Florida
Dennis A. Ross, Florida
Mark Walker, North Carolina
Rod Blum, Iowa
Jody B. Hice, Georgia
Steve Russell, Oklahoma
Glenn Grothman, Wisconsin
Will Hurd, Texas
Gary J. Palmer, Alabama
James Comer, Kentucky
Paul Mitchell, Michigan
Greg Gianforte, Montana

Elijah E. Cummings, Maryland, *Ranking Minority Member*
Carolyn B. Maloney, New York
Eleanor Holmes Norton, District of Columbia
Wm. Lacy Clay, Missouri
Stephen F. Lynch, Massachusetts
Jim Cooper, Tennessee
Gerald E. Connolly, Virginia
Robin L. Kelly, Illinois
Brenda L. Lawrence, Michigan
Bonnie Watson Coleman, New Jersey
Stacey E. Plaskett, Virgin Islands
Val Butler Demings, Florida
Raja Krishnamoorthi, Illinois
Jamie Raskin, Maryland
Peter Welch, Vermont
Matt Cartwright, Pennsylvania
Mark DeSaulnier, California
Jimmy Gomez, California

Sheria Clarke, *Staff Director*
William McKenna, *General Counsel*
Troy Stock, *Information Technology Subcommittee Staff Director*
Sean Brebbia, *Senior Counsel*
Kelsey Wall, *Professional Staff Member*
Sharon Casey, *Deputy Chief Clerk*
David Rapallo, *Minority Staff Director*

Subcommittee on Information Technology

Will Hurd, Texas, *Chairman*

Paul Mitchell, Michigan, *Vice Chair*
Darrell E. Issa, California
Justin Amash, Michigan
Blake Farenthold, Texas
Steve Russell, Oklahoma
Greg Gianforte, Montana

Robin L. Kelly, Illinois, *Ranking Minority Member*
Jamie Raskin, Maryland
Stephen F. Lynch, Massachusetts
Gerald E. Connolly, Virginia
Raja Krishnamoorthi, Illinois

Subcommittee on Intergovernmental Affairs

Gary Palmer, Alabama, *Chairman*

Glenn Grothman, Wisconsin, *Vice Chair*
John J. Duncan, Jr., Tennessee
Virginia Foxx, North Carolina
Thomas Massie, Kentucky
Mark Walker, North Carolina
Mark Sanford, South Carolina

Val Butler Demings, Florida, *Ranking Minority Member*
Mark DeSaulnier, California
Matt Cartwright, Pennsylvania
Wm. Lacy Clay, Missouri
(Vacancy)

CONTENTS

CYBERSECURITY OF VOTING MACHINES

Wednesday, November 29, 2017

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON INFORMATION TECHNOLOGY, JOINT
WITH SUBCOMMITTEE ON INTERGOVERNMENTAL AFFAIRS,
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM,
Washington, D.C.

The subcommittee met, pursuant to call, at 2:29 p.m., in Room 2154, Rayburn House Office Building, Hon. Will Hurd [chairman of the Subcommittee on Information Technology] presiding.

Present: Representatives Hurd, Palmer, Mitchell, Grothman, Duncan, Amash, Walker, Kelly, Demings, DeSaulnier, Lynch, Clay, and Krishnamoorthi.

Also Present: Representative Gabbard.

Mr. HURD. The Subcommittee on Information Technology and the Subcommittee on Intergovernmental Affairs will come to order. And, without objection, the chair is authorized to declare a recess at any time.

And now I am going to recognize myself for 5 minutes for my opening statement.

Good afternoon. Thanks for being here. And it's been over 240 years since our forefathers declared independence and our democratic experiment began. Throughout the entirety of our existence, our adversaries, both internal and external, have sought so suppress and destroy our democratic process.

Voting is one of our fundamental democratic rights and is the cornerstone of American democracy. Our existence as a democracy depends on free, fair, and accurate elections. Today, we're here to talk about the best way to protect the integrity of our voting systems through the cybersecurity of our voting machines and election systems.

There are over 10,000 election jurisdictions nationwide that administer elections, and even within States, counties use different systems and different technologies to conduct elections. A little over a year ago, last September. Ranking Member Kelly and I held a hearing in the IT Subcommittee entitled "Cybersecurity: Ensuring the Integrity of the Ballot Box." We discussed potential cybersecurity issues with the upcoming election. It was an issue then and it remains an issue now.

Former DHS Secretary Jeh Johnson has made clear that, to the best of his knowledge, the Russian Government did not, through any cyber intrusions, alter ballots, ballot counts, or reporting of election results. However, our adversaries have always sought to use our Nation's unique qualities to undermine our robust and resilient democracy.

Just because Russia did not tamper with ballots or reporting of election results during the last election, it doesn't mean they or other adversaries won't try to do so in the next election or the election after that. Like anything else in this the digital age, electronic voting is vulnerable to hacking. Our voting systems are no exception.

This past January, DHS designated the Nation's election systems as critical infrastructure, something that was being discussed at our hearing back in September of 2016. We are here today to follow up on what impact the designation has had on States. It is essential that States take appropriate steps to secure their voting infrastructure. It's also essential that States have the ability to audit their ballots for accuracy whenever any kind of manipulation is suspected.

The State of Virginia, which held an election recently, has joined the growing list of States that went to a paper system. I'm curious to hear how that transition went and what our witnesses think about moving to paper-based voting systems. Additionally, what are the chances that a foreign entity could tamper with the ballot box? These are all questions and issues that I want to explore today.

I'm very interested to hear what our witnesses have to say on this topic, and I thank the witnesses for being here today and for their efforts as fellow citizens to ensure that our country's elections are free and fair.

It's now a pleasure, I recognize the ranking member of the Information Technology Subcommittee, my friend, Ms. Robin Kelly, for 5 minutes in her opening remarks.

Ms. KELLY. Thank you, Mr. Chair. Welcome back. I hope you had a good Thanksgiving.

Thank you, Chairman Hurd and Palmer, for holding this important hearing today. There is no doubt that Russia, at the direction of President Vladimir Putin, attempted to manipulate our election and has worked to manipulate those of our western allies. It was a broad and coordinated campaign to undermine faith in democratic elections.

Earlier this year, the IT subcommittee explored the Kremlin's efforts to use social media to influence voters. Today, we are taking a look at another part of their effort to undermine our democracy by hacking our voting machines and election infrastructure.

More than 1 year ago, we held a hearing entitled "Cybersecurity: Ensuring the Integrity of the Ballot Box." During that hearing, we took a look at State and Federal preparations for any cyber attacks on our voting machines. Today, we have a clearer picture of what transpired, but we're still discovering new facts.

In September of this year, DHS notified 21 States that hackers affiliated with the Russian Government breached or attempted to breach their election infrastructure. In my home State of Illinois, the hackers illegally downloaded the personal information of 90,000 voters and attempted to change and delete data. Fortunately, they were unsuccessful.

While we continue learning about the full scope of Russia's election interference, one thing is clear: There will be another attempt to manipulate our elections, whether it be Russia, another nation state or a nonstate actor, even a terrorist organization. The threats to our election infrastructure are growing. So what are we going to do about it?

Earlier this year, researchers at the DEFCON conference successfully hacked five different direct recording electronic voting machines, or DREs, in a day. The first vulnerabilities were discovered in just 90 minutes. Even voting machines not connected to the internet still contained physical vulnerabilities like USB ports that can be used to upload malware.

Alarmingly, many DREs lack the ability to allow experts to determine that they have been hacked. Despite these flaws, DREs are still commonly used. In 2016, 42 States used them. They were more than a decade old, with some running outdated software that is no longer supported by the manufacturer. Updating our voting machines to audible, paper-based machines, such as optical scanners, is a step we need to take right now.

Our election infrastructure is broad and contain numerous vulnerabilities. If we are going to withstand a coordinated attack, we need a coordinated defense. In January of this year, DHS designated election infrastructure as critical infrastructure. In this announcement, then DHS Secretary Jeh Johnson was clear that this designation was not to be a Federal takeover of State and local election infrastructure. Rather, it was a designation intended to ensure that current State and local officials have the resources necessary to secure their elections.

Since then, former DHS Secretary and now White House Chief of Staff, General John Kelly, has supported this designation. This designation can help ensure that the cornerstone of our democracy, our elections, remain fair and secure. But if this designation is to be successful, we will all have to work together. DHS and our State election officials must do a better job of working together to detect and solve problems.

Again, I want to thank you, Mr. Chairman, for holding this crucial hearing. Thank you to our witnesses for being here. I look forward to hearing from all of you about how we can continue protecting our democracy.

I yield back.

Mr. HURD. It's always a pleasure to be with you, Representative Kelly.

I'd like to thank my friend, Chairman Palmer, for the Intergovernmental Affairs Subcommittee's cooperation and work on this important issue. And now it's a pleasure to recognize the ranking member of the Intergovernmental Affairs Subcommittee, Mrs. Demings, for 5 minutes in her opening remarks.

Mrs. DEMINGS. Thank you so much, Chairman Hurd and Chairman Palmer, for convening this hearing today. I'd also like to thank Ranking Member Kelly for her leadership, and all of our witnesses for joining us for this very important hearing.

I'm pleased that we're holding this hearing on a matter so essential to democracy. While there are many issues that divide us, the integrity of the voting process should not be in question. Regardless of race, gender, sexual identity, ZIP Code, income, every vote should count, every vote should count the same. I believe that voting is the last true equalizer.

However, Russia's interference in the 2016 election and intrusions in at least 21 State voter registration databases, indisputable and confirmed by U.S. intelligence agencies that forced us to acknowledge voting system security, has not kept pace with the current and emerging threats from nations, organizations, or even a single individual determined to undermine our democracy.

Recently, I joined the Congressional Task Force on Election Security. Just as we keep our homeland safe from physical harm, so too must we harden our soft targets against cyber attacks. The Task Force has heard from security professionals, academia, and State and local elections officials. Their message is clear: We must act now to protect our voting systems.

In over 40 States elections are carried out using voting machines and voter registration databases created more than a decade ago. These technologies are more likely to suffer from known vulnerabilities that cannot be patched easily, if at all. As we saw in the voting village setup at this year's DEFCON hacking conference, even hackers with limited prior knowledge, tools, and resources are able to breach voting machines in a matter of minutes. We should not assume that State voting machines are secure enough to withstand a state-sponsored cyber attack. And there is no reason to believe that these attacks will subside.

Congress must do its part—yes, we must—and help States fund and maintain security election systems. This means funding to purchase newer, more secure election systems and voting machines with voter-marked paper ballots, helping establish and certify baseline cybersecurity standards for those systems and the vendors that service them, and encourage States to conduct post-election risk limiting audits.

Our democratic process relies on voters' faith that their vote does count. Election security is national security, and our election infrastructure is critical infrastructure. With just under a year until the 2018 midterm elections, it is critical that we understand the vulnerabilities of the past and secure our networks for the future.

I thank our witnesses again for sharing their testimony today, and I look forward to this very important discussion. Thank you so much.

With that, I yield back.

Mr. HURD. Thank you, Ranking Member Demings.

And now I'm pleased to introduce our witnesses. First and foremost, the Honorable Christopher Krebs, the senior official performing the duties of the under secretary for National Protection and Programs Directorate at the U.S. Department of Homeland Security.

We have the Honorable Tom Schedler, Secretary of State for Louisiana. Thank you for coming up here today.

Commissioner Cortes, the commissioner on the Virginia Department of Elections. Sir, thank you for being here.

Dr. Matthew Blaze—excuse me—Blaze, associate professor of computer and information science at the University of Pennsylvania.

And Ms. Susan Klein Hennessey, a fellow in national security and governance studies at the Brookings Institute.

Welcome to you all. And pursuant to committee rules, all witnesses will be sworn in before you testify, so please rise and raise your right hand.

Do you solemnly swear or affirm the testimony you're about to give is the truth, the whole truth, and nothing but the truth?

Thank you.

Let the record reflect that all witnesses answered in the affirmative.

In order to allow time for discussion, please limit your testimony to 4 minutes. Your entire written statement will be made part of the record, and I appreciate you all's written statements, especially all of you all had, you know, outlined a number of interesting solutions to these problems, as well as articulating the concerns that we have. So folks that are interested in this topic, many of—all of these written statements is valuable in understanding the state of where we are.

As a reminder, also, the clock in front of you shows your remaining time. The light will turn yellow when you have 30 seconds left. And when it starts flashing red, that means your time is up. So please also remember to push the button to turn your microphone on before speaking.

And we'd like to start with Mr. Krebs. You are now recognized for 5 minutes—4 minutes, excuse me.

WITNESS STATEMENTS

STATEMENT OF HON. CHRISTOPHER C. KREBS

Mr. KREBS. Chairman Hurd, Chairman Palmer, Ranking Member Kelly, and Ranking Member Demings, and the members of the subcommittee, thank you for this opportunity to discuss the Department of Homeland Security's ongoing efforts to enhance the security of our elections.

In 2016, the United States saw malicious cyber operations directed against U.S. election infrastructure and political entities. Since January, we have reaffirmed the designation of election systems as critical infrastructure and the clear-eyed threats to our Nation's election systems remain an ongoing concern.

The organization I lead, the National Protection and Programs Directorate at the Department of Homeland Security, is leading an interagency effort to provide voluntary assistance to State and local officials. This interagency assistance brings together the Election Assistance Commission, the FBI, the intelligence community, NIST, and other DHS partners, and is modeled on our work with other critical infrastructure sectors.

Our Nation's election systems are managed by State and local governments in thousands of jurisdictions across the country. State and local officials have already been working individually and collectively to reduce risks and ensure the integrity of their elections. As threat actors become increasingly sophisticated, DHS stands up in—stands in partnership to support the efforts of election officials.

DHS offers three primary types of assistance: assessments, information, and incident response. DHS typically offers two kinds of assessments to State and local officials. First, the cyber hygiene service for internet-facing systems provides a recurring report identifying vulnerabilities in internet-connected systems and mitigation recommendations. Second, our cybersecurity experts can go onsite to conduct risk and vulnerability assessments. These assessments are more thorough and result in a full report of vulnerabilities and recommendations allowing the testing. As we continue to understand the requirements from our stakeholders, we'll refine and diversify these voluntary offerings.

In terms of information sharing, DHS continues to share actionable information on cyber threats and incidents through multiple means. For example, DHS published best practices for securing voter registration databases and addressing potential threats to election systems.

We share cyber threat indicators and other analysis that network defenders can use to secure their systems. The National Cybersecurity and Communications Integration Center, the NCCIC, works with the Multi-State Information Sharing and Analysis Center to provide threat and vulnerability information to State and local officials.

Election officials may also receive information and assistance directly from the NCCIC or through field-based cybersecurity advisors and protective security advisors. Notably, we're offering security clearances initially to senior election officials, and we're also exploring additional clearances to other State officials.

In our third category, the DHS's NCCIC provides incident response assistance to help State and local officials identify and remediate any possible incidents. In the case of an attempted compromise affecting election infrastructure, the NCCIC shares anonymized information with other States to assist their ability to defend their own systems in a collective defense approach.

It is important to note that these relationships are built and sustained on trust. Breaking that trust will have far-ranging consequences in our ability to collaboratively counter this growing threat.

To formalize and coordinate efforts with our Federal partners and election officials, we have established the Government Coordinating Council. We are similarly working to formalize partnerships with private sector industry through a sector coordinating council. Within this environment of sharing critical threat information, risk management, best practices, and other vital information, DHS is leading Federal efforts to support and enhance security across the Nation.

Securing the Nation's election systems is a complex challenge and a shared responsibility. There is no one size fits all solution. In conversations with election officials over the last year, in working with the EAC, NIST, DOJ, the Department has learned a great deal.

First, as you'll hear from Louisiana and Virginia, election officials already do great work. But like many other institutions in government and the private sector, resources remain a challenge. Not only budget for modernizing legacy IT, but also workforce training and recruitment around these critical skills. As we work collectively to address these and other challenges, the Department will continue to work with Congress and industry experts to support our State and local partners.

Thank you for this opportunity to testify, and I look forward to any questions.

[Prepared statement of Mr. Krebs follows:]

Written Testimony

of

Christopher Krebs
Senior Official Performing the Duties of the Under Secretary
National Protection and Programs Directorate
U.S. Department of Homeland Security

Before the
United States House of Representatives
Committee on Oversight and Government Reform
Subcommittees on Information Technology and Intergovernmental Affairs

Regarding
Cybersecurity of Voting Machines
November 29, 2017

Chairman Hurd, Chairman Palmer, Ranking Member Kelly, Ranking Member Demings and members of the Subcommittees, thank you for inviting me to participate in today's hearing on securing our elections from malicious cyber activity. This is an especially timely topic given the elections earlier this month. As you know, the Department of Homeland Security (DHS) performs a critical mission focused on reducing and eliminating threats to the nation's critical physical and cyber infrastructure, including how it relates to our elections.

Given the vital role that elections play in a free and democratic society, the Secretary of Homeland Security determined that election infrastructure should be designated as a critical infrastructure subsector. With the establishment of an Election Infrastructure Subsector (EIS), the DHS National Protection and Programs Directorate (NPPD) and federal partners have been formalizing the prioritization of ***voluntary*** cybersecurity assistance for election infrastructure similar to that which is provided to a range of other critical infrastructure entities, such as financial institutions and electric utilities.

During the 2016 election period and since that time, the federal government and election officials have been meeting regularly to share cybersecurity risk information and to determine effective means of assistance. Recently, the EIS Government Coordinating Council (GCC) met to establish goals and objectives, to develop plans for the EIS partnership, and to lay the groundwork for developing an EIS Sector Specific Plan (SSP). The GCC framework provides a well-tested mechanism across critical infrastructure sectors for sharing threat information between the federal government and council partners, advancing risk management efforts, and prioritizing services available to sector partners in a trusted environment. EIS-GCC representatives include DHS, the U.S. Election Assistance Commission (EAC), the National Institute of Standards and Technology (NIST), the Federal Buruea of Investigation (FBI), the Department of Defense (DoD), and key state and local election officials. Participation in the council is entirely voluntary and does not change the fundamental role of state and local jurisdictions in overseeing elections.

In addition to the work of the EIS-GCC, DHS continues to engage state and local elections officials – coordinating requests for assistance, risk mitigation, information sharing, and incident coordination resources and services. In order to ensure a coordinated approach across DHS, NPPD has brought together stakeholders from across the Department as part of an Election Task Force (ETF). The ETF increases the Department's efficiency and efficacy in understanding, responding to, communicating, and sharing information related to cyber threats. The ETF serves to provide actionable information to assist states in strengthening their election infrastructure against cyber threats.

Assessing the Threat

DHS continues to robustly coordinate with the EAC, the intelligence community, and law enforcement partners. Among non-federal partners, DHS has been engaging state and local officials, as well as relevant private sector entities, to assess the scale and scope of malicious cyber activity potentially targeting the U.S. election infrastructure. In addition to working directly with state and local officials, we partnered with stakeholders to analyze relevant cyber data, including the Multi-State Information Sharing and Analysis Center (MS-ISAC), the

National Association of Secretaries of State and the National Association of State Election Directors.

We also used our field personnel deployed around the country, to help further facilitate information sharing and enhance outreach. Such engagement paid off in terms of identifying suspicious and malicious cyber activity targeting the U.S. election infrastructure. A body of knowledge grew throughout the summer and fall of 2016 about suspected Russian government cyber activities, and understanding that helped drive collection, investigations, and incident response activities. On October 7, 2016, DHS and the Office of the Director of National Intelligence (ODNI) released a joint statement to the public on election security and urged state and local governments to be vigilant and seek cybersecurity assistance.

We continue to assess that mounting widespread cyber operations against U.S. voting machines at a level sufficient to affect a national election would require a multiyear effort with significant human capital and information technology (IT) resources available only to nation-states. The level of effort and scale required to significantly change a national election result, however, would make it nearly impossible to avoid detection.

Enhancing Security for Future Elections

DHS continues to focus our efforts on ensuring a coordinated response from DHS and its federal partners to plan, prepare, and mitigate risk to the election infrastructure. We recognize that working with stakeholders is the only sure way to ensure more secure elections. Based on our assessment of activity observed in the last election, DHS is engaged with stakeholders across the spectrum to increase awareness of potential vulnerabilities and enhance security of U.S. election infrastructure.

Our election process is governed and administered by state and local election officials in thousands of jurisdictions across the country. These officials manage election infrastructure and ensure its security on a day-to-day basis. State and local election officials across the country have a long-standing history of working both individually and collectively to reduce risks and ensure the integrity of their elections. In partnering with these officials through both new and existing, ongoing engagements, NPPD is working to enhance their efforts to secure election systems.

Improving coordination with state and local partners: Increasingly, the nation's election infrastructure leverages IT for efficiency and convenience. Similar to other IT systems, reliance on digital technologies introduces new cybersecurity risks. NPPD helps stakeholders in federal departments and agencies, state and local governments, and the private sector to manage some of these cybersecurity risks. Consistent with our long-standing partnerships with state and local governments, we have been working with election officials to share information about cybersecurity risks, and to provide voluntary resources and technical assistance.

DHS works with the MS-ISAC to provide threat and vulnerability information to state and local officials. Created by DHS over a decade ago, the MS-ISAC is partially funded by NPPD. The MS-ISAC's membership is limited to state and local government entities, and all fifty states and US territories are members. It has representatives co-located with the NCCIC to enable regular collaboration and access to information and services for state chief information officers.

Providing technical assistance and sharing information: Through engagements with state and local election officials, including working through the Sector Coordinating Council, NPPD actively promotes a range of services to include but are not limited to the following:

Cyber hygiene service for Internet-facing systems: This voluntary service is conducted remotely, afterwards, NPPD provides state and local officials with a report identifying vulnerabilities and mitigation recommendations to improve the cybersecurity of systems connected to the Internet, such as online voter registration systems, election night reporting systems, and other Internet-connected election management systems. During the 2016 election, we provided cyber hygiene services to 33 state and 36 local election jurisdictions.

Risk and vulnerability assessments: These assessments are more thorough and executed on-site by NPPD cybersecurity experts. These evaluations require two to three weeks and include a wide range of vulnerability testing services, focused on both internal and external systems. When NPPD conducts these assessments, we provide a full report of vulnerabilities and recommended mitigations following the testing. These assessments are available on a limited, first-come, first-served basis.

Incident response assistance: We encourage state and local election officials to report suspected malicious cyber activity to the NCCIC. On request, the NCCIC can provide on-site assistance in identifying and remediating a cyber incident. Information reported to the NCCIC is also critical to the federal government's ability to broadly assess malicious attempts to infiltrate election systems. This technical information will also be shared with other state officials so they have the ability to defend their own systems from similar malicious activity.

Information sharing: DHS will continue to share relevant information on cyber incidents through multiple means. The NCCIC works with the MS-ISAC, and election officials can connect with the MS-ISAC or their State Chief Information Officer directly as one way to benefit from this partnership and rapidly receive information they can use to protect their systems. State election officials may also receive incident information directly from the NCCIC. In 2016, best practices, cyber threat information, and technical indicators, some of which had been previously classified, were shared with election officials in thousands of state and local jurisdictions.

Classified information sharing: DHS provides classified briefings to cleared stakeholders upon request, as appropriate and necessary.

Field-based cybersecurity advisors and protective security advisors: DHS has more than 130 cybersecurity and protective security personnel available to provide actionable information and connect election officials to a range of tools and resources to improve the cybersecurity preparedness of election systems and to secure the physical site security of voting machine storage and polling places. These advisors are also available to assist with planning and incident management for both cyber and physical incidents.

Physical and protective security tools, training, and resources: NPPD provides advice and tools to improve the security of polling sites and other physical election infrastructure. This guidance can be found at www.dhs.gov/hometown-security. This guidance helps to train administrative and volunteer staff on identifying and reporting suspicious activities, active shooter scenarios, and what to do if they suspect an improvised explosive device. Officials can also contact local NPPD PSAs for access to DHS resources.

2017 Elections and Beyond

This hearing is timely given the elections earlier this month. We have been working with election officials in all states to enhance the security of their elections by volunteering operations support and by establishing essential lines of communications with election infrastructure partners at all levels – public and private – for reporting both suspicious cyber activity and incidents. To quickly and effectively evaluate and triage any potential cyber-related events related to Election Day, DHS enhanced its state of readiness. Our goal was to enhance transparency and have visibility of aggregated elections-related cybersecurity efforts. These enhanced operations exercised interagency coordination, incident escalation, and incident communications to better improve guidance and planning in preparation for elections operations in 2018 and beyond.

In closing, the fundamental right of all citizens to be heard by having their vote accurately counted is at the core of our American values. Ensuring the integrity of our electoral process is a vital national interest and one of our highest priorities as citizens in a democratic society. We have confidence in the overall integrity of our electoral system. Our voting infrastructure is diverse, subject to local control, and has many checks and balances. As the threat environment evolves, the Department will continue to work with state and local partners to enhance our understanding of the threat; and to provide essential physical and cybersecurity tools and resources available to the public and private sectors to increase security and resiliency.

Thank you for the opportunity to appear before the Subcommittees today. I look forward to your questions.

Mr. HURD. Thank you, Mr. Krebs.

And, Secretary Schedler, again, I want to thank you for being flexible. I know this has been rescheduled a few times, but your perspective and experience on this topic is important, and thank you for being here. And, sir, you're now recognized for 4 minutes.

STATEMENT OF HON. TOM SCHEDLER

Mr. SCHEDLER. Thank you, Mr. Chairman, and thank you to this committee for the invitation to participate today.

It's important for you to hear the perspective of those who oversee elections across the country. My perspective comes from serving as Louisiana's Secretary of State since 2010, and past president of the National Association of Secretaries of State, or NASS, which represents a majority of the Nation's chief election officials.

Securing elections in the November 2018 and beyond is critical and important to all of us and our Nation's secretaries of state. We are not naive to the likelihood of future cyber attacks, but we also know the use of paper ballots can just as easily open up fraud vulnerabilities unless strong protocols are followed by election officials. That's why all 50 States continue to prepare accordingly.

First, I'd like to share with you the important developments taking place through NASS Election Cybersecurity Task Force, which was established in February of this year. This is a bipartisan body of the Nation's chief election officials. In addition to helping States share information and combat cyber threats, the task force assists in creating partnerships with public-private stakeholders, including the U.S. Department of Homeland Security and the U.S. Election Commission as well.

NASS has been a key player in the development of new Election Infrastructure Coordinating Council. This council is required as a result of the new designation for elections as critical infrastructure. The Council is designated or designed to facilitate improved communications that, as you know, did not go extremely well in 2016. NASS opposed the critical infrastructure designation because our members were concerned about the possibility of Federal overreach and because the designation came without meaningful consultation with any election officials.

My colleagues and I understood that we could continue to get the same support and services from DHS without critical infrastructure designation. So it seemed unnecessary. However, the designation is still with us today, and we have made good-faith efforts to work together with DHS. Part of that work includes chief election officials obtaining security clearances. We have often been told by DHS that they can't share information because it is clarified—classified, excuse me. Hopefully, these new clearances will address this problem.

Ensuring the integrity of the voting process is central to the role of every chief elections officer, including myself. And as some examples, in Rhode Island, Secretary Nellie Gorbea, convened over 100 election and IT officials for a cybersecurity summit. In West Virginia, Secretary Mac Warner has added an Air National Guard cybersecurity specialist to his staff. Vermont Secretary of State Jim Condos solicited a third party risk assessment of data systems in 2015 that lead to his office to build a new firewall and began regular penetration testing. Colorado Secretary Wayne Williams' office provides end point protection software for counties to install on their computers to detect viruses and malware functions.

And many States have or are developing disaster preparedness and recovery plans that include strategies on election systems and data are disrupted. In Louisiana, our hurricane season, we are one of those States for sure that is very expert in that field.

In terms of voting machines security, you remember that with the passage of the Help America Vote Act in 2002, States were required to purchase at least one piece of accessible voting equipment for each polling place. The Election Assistance Commission and the National Institute on Standards and Technology began updating the existing voting system or guidelines to address new systems such as DREs.

Last month, the EAC released their latest update to volunteer voting systems guidelines. The guidelines are set for manufacturing specifics that are certain standards of functionality, accessibility, accuracy, audibility, and security capabilities. And final approval by EAC is expected in the spring of 2018.

In Louisiana, we take pride and go way beyond any current standards with our voting machines. We are a top down State. The State purchases, warehouses every voting machine in the State. Additionally, we have the most current software available in all of our voting machines, and we test each and every one before and after elections. Once the machines are tested, a tamper-proof seal is placed on them to protect against any intrusion.

In Louisiana, because no one touches our voting machines except our staff, because they are never sent out to a manufacturer for repair, they are not handled by individuals or companies who program voting machines because they are readily tightly controlled by our office. We have the utmost of confidence in the system.

We do need to prepare. Yes. We do need to continue to update our processes and procedures. Yes. We do need to be vigilant. Yes. As secretaries of state, at NASS, we are currently looking for better practices that we can solicit from various entities and groups. And most of all, we're looking for the remaining $396 million in Federal HAVA that we have never been appropriated to help us replace aging equipment purchased over 10 years ago.

I'll certainly be available for any questions.

[Prepared statement of Mr. Schedler follows:]

Statement from the

Honorable Tom Schedler

Louisiana Secretary of State

Former President, National Association of Secretaries of State (NASS),
Co-Chair, NASS Elections Committee

Member, NASS Election Cybersecurity Task Force

Before the U.S. Subcommittee on Information Technology and
Subcommittee on Intergovernmental
Affairs of the House Committee on Oversight and Government
Reform

Cybersecurity of Voting Machines

November 29, 2017
Washington, DC

National Association of Secretaries of State
444 North Capitol Street, NW – Suite 401
Washington, DC 20001
202-624-3525 Phone/202-624-3527 Fax
www.nass.org

Hon. Tom Schedler, Louisiana Secretary of State
Statement Before the U.S. House of Representatives
November 29, 2017 | Washington, DC

NASS
National Association
of Secretaries of State

Securing elections occurring this November, in 2018, and beyond are of critical importance to our nation and our Secretaries of State. We are not naïve about the likelihood of future cyberattacks against digital elements of election systems, but we also know paper ballots include fraud vulnerabilities as well unless proper procedures and protocols are adopted and followed by election officials. That is why all 50 states continue to prepare accordingly.

Chief state election officials and their staff are constantly evaluating and developing programs to safeguard the integrity of their elections systems. In the last year-plus, those efforts have largely focused on the latest form of potential fraud--cyberattacks. My perspective comes from serving as Louisiana Secretary of State and past president of the National Association of Secretaries of State, or NASS, which represents a majority of the nation's chief state election officials. I also serve as the current co-chair of the NASS Elections Committee, and a member of the NASS Election Cybersecurity Task Force. Most recently, I was also appointed by NASS to serve as one of eight (8) Secretaries on the newly formed Election Infrastructure Subsector Government Coordinating Council.

Let me begin by thanking this Committee and Chairman Hurd for the invitation to participate today. It is important for you to hear the perspective of those who oversee elections across the country. First, I'd like to address the important developments taking place through the NASS Election Security Task Force.

NASS Election Security Task Force

The NASS Election Security Task Force was established in February 2017. This is a bipartisan body of the nation's chief state election officials. The mission of the Task Force is to promote the unique priorities and challenges that exist regarding cybersecurity and elections. In addition to helping states share information and combat cyber threats, the Task Force is charged with providing guidance on NASS efforts to create partnerships with public/private stakeholders, including the US Department of Homeland Security (DHS) and the US Election Assistance Commission (EAC). For example, the Task Force regularly works with elections and cybersecurity experts like the Center for Democracy and Technology, the Democracy Fund, and Harvard's Belfer Center plus other organizations looking to provide support and advice.

NASS has been a key player in the development of the new Election Infrastructure Subsector Coordinating Council (EIS-GCC). This "Council" is required as a result of the new designation for elections as critical infrastructure. Over the past several months we have worked with other state and local election official organizations as well as DHS and the EAC to try to make this "Council" function for a critical infrastructure sector that is really unlike any other. Instead of being chaired by a federal agency, it will be run by an Executive Committee of federal, state and local officials.

The "Council" is designed to facilitate improved communications between federal, state and local officials on threats and vulnerability information which as you know, did not go extremely well in 2016. The "Council" will meet numerous times over the next year to establish communication protocols for threat sharing and notification. The goals are to fine-tune DHS resources and tools available for state and local governments, and to discuss and review cyber best practices for sharing with state and local election officials.

In full transparency, NASS opposed the Critical Infrastructure designation in February 2017 because our members were concerned about the possibility of federal overreach and because the designation came without meaningful consultation with any election officials. My colleagues and I understood that we could continue to get the same support and services from DHS without a Critical Infrastructure designation, thus it seemed an unnecessary and overly burdensome and bureaucratic move. However, the designation is still with us and we have made a good faith effort to work together with DHS to improve lines of communications on election cybersecurity issues.

Part of these improved communications includes our successful lobbying for chief state election officials to obtain security clearances. We have often been told by DHS that they can't share some piece of information because it is classified. Hopefully, these new clearances will address this problem. DHS is also working to secure two additional clearances for staff designated by the Secretary of State. This will help to turn classified information into actionable information that states can employ to further protect their systems.

Innovative Cybersecurity Initiatives at the State Level

Ensuring the integrity of the voting process is central to the role of the chief state election official. Allow me to share with you some of the ways we are working hard to bolster election cybersecurity in the states:

Hosting State Cybersecurity Summits for Elections/IT Officials: In conjunction with the Rhode Island State Board of Elections, Secretary of State Nellie M. Gorbea recently convened over 100 local elections and IT officials for a Cybersecurity Summit at Salve Regina University in Newport, Rhode Island.

The three-hour forum highlighted national conversations around elections and cybersecurity and trained attendees on best practices to help keep these systems secure. Secretary Gorbea noted that Rhode Island has modernized its elections infrastructure over the past three years.

Leveraging National Guard Cybersecurity Expertise: In West Virginia, Secretary Mac Warner has added an Air National Guard cybersecurity specialist to his office staff.

The specialist holds top security clearance in the Air National Guard and will assess the state's elections systems and cybersecurity defenses. The specialist is embedded in the state's Fusion Center, which anticipates, prevents, and monitors criminal and terrorist activity in the state. The Fusion Center, the state's Division of Homeland Security and Emergency Management, and the National Guard are all part of West Virginia's Department of Military Affairs and Public Safety.

Several other states work with the National Guard on a variety of exercises to improve their cyber posture. For example, the Colorado National Guard's Defensive Cyber Support team works with the Secretary of State's cyber team to monitor online voter registration system activity. They are prepared to assist if cybersecurity incidents occur. In Ohio, the National Guard's cyber unit conducts penetration tests to check the state elections system for vulnerabilities or malicious activity. And in states like Rhode Island, the Secretary of State incorporates the National Guard in their statewide cybersecurity training for elections and IT officials.

Initiating Third-Party Risk Assessment of Electronic Data System: Vermont Secretary of State Jim Condos solicited a third-party risk assessment of its physical and electronic data systems in 2015. The process led his office to build new firewalls around several of its web applications and to begin regular penetration testing.

Vermont, along with many other states, also conducts audits within 30 days of each election. Votes are recounted in a sampling of precincts to reveal any discrepancies between the paper ballots and Election Day tallies. New risk-limiting audits are beginning in Colorado this November and a handful of states around the country have recently passed legislation to employ this practice. We will be watching and learning from these states as other states begin to pursue activity like this.

Assisting the Locals

Secretaries of State have a strong, pre-existing relationship with local election officials. Colorado's office provides endpoint protection software for counties to install on their computers to detect virus and malware infections.

Advanced malware detection software like Malwarebytes, BitDefender, and Crowdstrike can help prevent infection of computers by phishing attacks and provide monitoring in order to assist in reacting and responding to events quickly.

Additionally, the Colorado Secretary's staff provide cyber cross-training and audits for county elections staff. They also conduct yearly tests for county staff who interact with state voter registration systems and require them to adhere to state security standards.

Other Cybersecurity Initiatives Involving One or More States:

Establishing State Cybersecurity Task Forces: Many Secretaries and Governors have established state cybersecurity task forces, which provide the opportunity to share information with other state and local officials on overall cybersecurity efforts and those specific to elections.

Working with the Multi-State Information Sharing and Analysis Center (MS-ISAC): The mission of the MS-ISAC is to improve the cybersecurity posture of the nation's state, local, tribal and territorial governments through focused cyber threat prevention, protection, response, and recovery.

Seven states are working with MS-ISAC on a pilot project to develop an elections-specific ISAC. This will enable more targeted information for state elections officials as they partner with MS-ISAC. The seven states participating in this pilot project are: Colorado, Indiana, New Jersey, Texas, Virginia, Vermont, and Washington.

Retaining, Updating Security Tools and Procedures. States are constantly adding new cybersecurity tools and procedures. These include the use of dual or multifactor authentication; strengthened data encryption; improved data classification to monitor different types of threats; enhanced tracking of worker access to data; use of data access cards; statistical analysis of data patterns, including artificial intelligence analysis of logs; launching Google Shield; and reviewing procedures to minimize potential unauthorized physical access to machines.

Creating Incident Response Plans. States have Emergency Preparedness Plans for Elections, and these plans now include cyber incident responses. Some have or are developing disaster recovery plans that include strategies when election systems and data are disrupted. Table top exercises are also included incident response plans. The exercises test emergency procedures and communications.

Monitoring Social Media Accounts: As Election Day approaches, some states monitor their office's social media with increased scrutiny. They note any increased use of certain terms on Facebook or Twitter that indicate potential meddling in the election process. By picking up on these terms quickly, they are able to react instantly, heading off any orchestrated attempt to influence the election via social media.

The Security of Voting Systems

With the passage of the Help America Vote Act in 2002, states were required to purchase at least one piece of accessible voting equipment for each polling place. Back in 2002, the accessible equipment available to purchase were Direct Recording Electronic Equipment (DRE's). The Election Assistance Commission and the National Institute for Standards and Technology (NIST) began updating the existing voting system guidelines to address these new systems. They have been updated in full or in part only a handful of times since then.

Just last month, the EAC released their latest draft of the Voluntary Voting System Guidelines (VVSG 2.0). The guidelines are a set of manufacturing specifications that voting systems can be tested against to determine if they meet certain standards of functionality, accessibility, accuracy, auditability and security capabilities. VVSG 2.0 have been approved by the EAC's Technical Guidelines Development Committee (TGDC) and is currently going through a public comment period. The next step will be consideration by the EAC Board of Advisors and Standards Board and final approval by the EAC Commissioners which is expected in the Spring of 2018.

In Louisiana, we take pride that we go above and beyond in following best practices in terms of our voting machines. We are a top down state: the state purchases, controls, stores, repairs, and programs all of the voting machines across the state. Additionally, we have the most current software available on all of our voting machines, and we test each and every one before and after the election. Once the machines are tested, a tamper proof seal is placed on them to protect against any intrusions.

Let's face it: not all counties and municipalities in a state are set up this way so we are not necessarily equal. But in Louisiana, because no one touches our voting machines except our staff; because they are never sent out to the manufacturer for repairs; because they are not handled by individuals or companies who program voting machines and; because they are very tightly controlled by our office and our office alone, I have the utmost confidence in our vote tallies. In fact, in many ways, our machines are overwhelmingly trusted by our voters when compared to their confidence in the security of mailed, paper ballots.

The bottom line is, because the State of Louisiana purchases and maintains all of our voting machines even a poor parish (county) can have just as secure an experience on Election Day as a wealthy one. That's the definition of a fair and impartial election.

My conclusion, after more than a year of intense questioning of my own staff and experts, is: we believe we have the most up-to-date and effective processes and procedures in place to keep our voting machines safe and operational. Machines that have been hacked at attention-grabbing conferences like DEFCON do not take into account any of the security/safety measures I just outlined and are not set up in real world election environments by any stretch of the imagination. To me, that is not an accurate test or a level playing field.

Since the Presidential Election of 2016, my staff have managed five elections. Absent the hype about Russian hacking, we have received no complaints from voters at all about the performance or accuracy of our voting machines. None.

Do we need to be prepared? Yes. Do we need to continue to update our processes and procedures? Yes. Do we need to vigilant? Yes. Each state has to decide for itself how best to secure their citizens' election system. Louisiana is not a same day/automatic voter registration state. Louisiana only uses paper ballots for absentee voters, so it is quite limited. Louisiana does have a Photo I.D. law that has been in place since 1997 and is well accepted by voters. These choices have protected the integrity of our election systems in Louisiana very well.

As Secretaries of State we look to NASS for additional guidance on best practices for cybersecurity from groups like the EAC and NIST. We are looking to DHS for clearance so we can receive classified information on credible threats to mitigate our risks. Most of all, we are looking for the remaining $396 million federal HAVA dollars that have never been appropriated to help us replace aging equipment purchased over ten years ago. These are the real needs to secure our election cybersecurity going forward.

Thank you for this opportunity to comment.

Mr. HURD. Thank you, sir.

And, Commissioner Cortes, I'd like the record to reflect that you were prepared to come testify the day after your most recent elections, and I appreciate your willingness to address this body. And, sir, you're now recognized for 4 minutes.

STATEMENT OF HON. EDGARDO CORTES

Mr. CORTES. I'm Edgardo Cortes. I'm the Commissioner of Elections in Virginia. In this role, I serve as the chief election official for the Commonwealth, and I lead the Virginia Department of Elections.

Virginia has 133 local election jurisdictions and over 5 million active registered voters.

So you have my written remarks, and today I'm going to focus on the recommendations that I provided in there.

During my tenure, the Department has focused on using technology to create a better voting experience for eligible Virginians, and reduce the administrative workload for local election officials, while increasing security and accountability in our processes.

As part of the McAuliffe administration's focus on cybersecurity, one aspect of the these wide-ranging efforts has been to strengthen the security and reliability of Virginia's voting equipment, including the voting machines and the electronic pollbooks used to administer elections in the Commonwealth.

When I became commissioner in 2014, approximately 113 of Virginia's 133 localities used paperless DREs that were over a decade old and already past their expected end of life. I'm happy to say that all Virginians voted using a paper-based system in the November 2017 general election.

Virginia has twice been put in the unfortunate position of having to decertify voting equipment and transition to new equipment in a condensed timeframe based on security concerns, previously used DREs. These steps, outlined in detail in my written testimony, were not taken lightly. They placed a financial and administrative stress on the electoral system. They were, however, essential to maintain the public's trust and the integrity of Virginia elections.

The November 2017 general election was effectively administered without any reported voting equipment issues. Thanks to the ongoing partnership between the State, our hardworking local election officials, and our dedicated voting equipment vendors, the transition to paper-based voting systems on a truncated timeline was incredibly successful and significantly increased the security of the election.

Although it's clearly possible to transition quickly, doing so is less than ideal. I request that you consider the following recommendations, which I believe will make these issues much easier to manage in the future.

Number one, Congress needs to ensure sufficient Federal funding is available for States to procure and maintain secure voting equipment and increase security of all election systems. This is a critical need and must be addressed immediately if the funding is going to provide any assistance in time for the 2018 midterm elections.

Number two, the U.S. Election Assistance Commission has been critical to ensuring that a baseline set of standards for voting systems, adequate testing protocols, and certified test labs are available to States. Congress must ensure the EAC is fully funded so they can continue to be an exceptional resource to State and local officials.

Number three, Congress should ensure the use of or—to ensure the use of secure voting equipment in the future, Congress should require Federal certification of all voting systems used in Federal elections. This is currently a voluntary process. Federal certification should also be required for electronic pollbooks, which currently are not subject to any Federal guidelines. Requiring Federal certification for both of these will ensure there is a security baseline for use across the country to ensure the integrity and security of our elections.

And finally, Congress should establish some sort of accreditation system for election administrator training to ensure that the individuals responsible for this fundamental American right are equipped with the appropriate skill and knowledge set. Elections are an integral function of government, and we still have much more to do in Virginia and across the country to secure our election infrastructure from potential threats, especially with the midterm elections quickly approaching.

While we're extremely appreciative of the work and assistance provided by the EAC and DHS to date, the Federal Government can and should do more to assist States in safeguarding this most fundamental American right.

Thank you again for inviting me to join you today and your interest in hearing from election administrators about the work being done to secure the Nation's voting systems. We look forward to continuing to work with Congress to ensure sufficient Federal resources are available to State and local election officials to continue this important work. Thank you.

[Prepared statement of Mr. Cortes follows:]

SUBCOMMITTEE ON INFORMATION TECHNOLOGY AND THE SUBCOMMITTEE ON INTERGOVERNMENTAL AFFAIRS OF THE COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

TESTIMONY OF
EDGARDO CORTÉS
COMMISSIONER
VIRGINIA DEPARTMENT OF ELECTIONS

NOVEMBER 29, 2017

I. Introduction

Good morning. I appreciate the invitation to speak with you today. My name is Edgardo Cortés, and I am the Commissioner of Elections in Virginia. In this role, I serve as the Chief Election Official for the Commonwealth and lead the Department of Elections. Virginia has 133 local election jurisdictions and over 5 million active registered voters. During my tenure, the Department has focused on using technology to create a better voting experience for eligible Virginians and reduce the administrative workload for local election officials while increasing security and accountability in our processes.

We have done much work in this arena, and one aspect of these wide-ranging efforts has been to strengthen the security and reliability of Virginia's voting equipment, including the voting machines and electronic pollbooks that I have been asked to discuss today. Our most recent action to protect and secure elections in Virginia was the decertification of all direct-recording electronic voting machines("DREs") on September 8, 2017, approximately 59 days prior to our General Election. This step was not taken lightly, and it placed financial and administrative stress on the electoral system. It was, however, essential to maintain the public's trust in the integrity of Virginia elections. This administration and the Virginia election community have faced many challenging situations in the past four years. We addressed this situation as we did each of the others: with a solid determination to ensure that eligible Virginians were able to vote with confidence.

We have much more to do. While we are extremely appreciative of the work and assistance provided by the U.S. Election Assistance Commission (EAC) and the U.S. Department of Homeland Security (DHS), the restrictions placed on these entities, including financial and legal restrictions, limit the assistance that they can provide to Virginia and other state election officials as we face attacks from other nation states, hackers of all stripes and an ever-changing security environment with minimal resources. To the extent that elections are an integral function of government, the federal government can and should do more to assist states in safeguarding this most fundamental American right.

II. Virginia Election Administration Ecosystem Overview

The Virginia election administration ecosystem is structured comparably to several other states in that local officials administer and mostly pay for elections, and the state supervises and coordinates this work and ensures uniformity. Regarding voting equipment specifically, the state is responsible for certifying voting equipment, such as DREs and electronic pollbooks; local officials are responsible for choosing their equipment from the state menu of certified options. Our state certification requirements voluntarily rely on the existing federal criteria and once a system is certified, no additional testing is currently required by the state to retain certified status.

From a security standpoint, this top-down structure has proved exceptionally important – specifically for the creation and maintenance of strong and sustainable security systems for our statewide voter registration database (Virginia Election & Registration Information System, or VERIS). In this area, the local officials are responsible for processing individual voter registration applications and making determinations related to eligibility; the state is responsible for the aggregation, security and proper handling of all information entered by the locals about individual voters. The state also is responsible for collecting and managing the information from a myriad of other non-election agencies and entities, such as death records from the U.S. Social Security Administration, conviction information from federal courts and voter registrant information from other states. Local officials are responsible for reviewing the individual records that the state has identified as possible matches to voters in their localities.

In this manner, the state efficiently uses its resources so that each of the 133 localities doesn't have to procure individual voter file software packages, individual information technology staff members and security experts to conduct routine list maintenance.

III. WINVote Decertification

When I became Commissioner in 2014, approximately 113 of Virginia's 133 localities used paperless DREs that were over a decade old and already past their expected end of life. The first map you have provides an overview of DRE usage in Virginia at that point. State legislative efforts to curtail the use of the machines had been ineffective, and complaints related to this equipment were increasing. To address these problems, Governor McAuliffe proposed $28 million in the state budget for new voting equipment during the 2015 legislative session. Unfortunately, the General Assembly refused and left financial responsibility for new voting equipment with local officials.

In response to DRE issues in the 2014 election, such as those experienced by supporters of your former colleague, Congressman Rigell in Virginia Beach, the Department conducted a review of the reported 2014 voting equipment complaints. During that review, the Department discovered that one of the certified DRE machines, the WINVote, was operating while its wireless network was turned on. With no prior state decertification history to rely on, I asked the state IT department (Virginia Information Technologies Agency, or VITA) to assess the equipment's security. Even with no voting equipment experience, a staff member was able to manipulate a WINVote machine that was located in one office while she was sitting in a different office down the hall. This discovery necessitated immediate action. The June Primary Election was a few short months away and the approximately 30 localities using WINVote machines, which accounted for about 20 percent of precincts in the state, had no money in their local budgets for the immediate procurement of new voting equipment.

The Department contacted the affected localities and informed them of the potential impending decertification. We also contacted the organizations representing local officials and the voting equipment vendors, which promptly confirmed sufficient inventory and capacity to immediately equip the localities with new machines. The vendors, in competing for each affected locality's business, offered creative financial incentives.

In response to VITA's findings, the WINVote was decertified 55 days prior to the 2015 June Primary in spite of many comments predicting "certain failure," which I assume are similar to comments you've received about concerns with transitioning voting equipment. With lots of teamwork, the June Primary Election was administered without issue related to the new voting equipment. The most important factors in this successful transition were the partnerships with the individuals and entities mentioned above and the ongoing and constant communications with all interested parties.

IV. September 2017 Decertification

As part of the McAuliffe administration's focus on cybersecurity, the Department of Elections has been focused on strengthening the security of our voting processes during the past four years, including encouraging remaining localities using paperless DREs to transition to new equipment as quickly as possible. In the wake of the WINVote decertification, almost every locality with sufficient financial resources had procured new voting equipment; however, there were several localities that continued to use one of the approximately five different DRE models still certified in Virginia. The Department learned that DEF-CON, the annual hacker conference held in Las Vegas, planned a "Voting Village" exhibit at their July conference. The public reporting from DEF-CON created substantial security concerns. When my CIO alerted me that a DEF-CON attendee posted the password for one of the voting systems in use in Virginia, I knew immediate action was necessary in advance of the upcoming election. The second map you have represents DRE usage at that point.

As you can see, there were only about 30 localities that had not updated their voting equipment and were still using one of five old DRE voting systems, such as the Sequoia Edge and the TSX Accuvote. What this map also shows are the real consequences of the decision to not provide federal or state funding for equipment: generally, only the poorer and more rural localities were forced to continue to use antiquated and problematic voting machines because they couldn't afford new ones.

While we knew that a transition was possible because of prior experience, this decertification faced some slightly different challenges. For example, we now needed testing done on five *different* voting systems, yet the state had no way to compel the vendors or localities to provide equipment for VITA testing. Through relationships with the locals, we obtained equipment for all but one type of system: the Hart eSlate. The vendor also refused to provide the equipment. This was a big problem.

On the other hand, we also had additional helpful partners for this decertification. While the equipment was being tested, but before the official decertification, the Voter Registrars Association of Virginia ("VRAV") wrote to its membership. VRAV expressly acknowledged that any voting equipment almost two decades old was unlikely to withstand any review under today's IT security standards, and officially recommended that all localities move forward immediately with obtaining new equipment. Verified Voting also served as a resource and provided the Department and VITA, under exceptionally tight timelines, with helpful information about the equipment's vulnerabilities.

Approximately 10 weeks prior to the 2017 November General Election, VITA provided preliminary information related to the machines, which was very concerning. When reviewing the Department's options, the Department asked whether VITA would be willing to confirm the accuracy of results cast on any of the machines in the event that future election results were called into question. In response, VITA asserted that they would not, at that time, be willing to provide unqualified statements of support. The next week, 59 days prior to the election, all DREs were decertified. All affected localities promptly obtained new voting equipment and in-person absentee voting began, as scheduled, approximately two weeks after the decertification and was conducted without incident related to the new voting equipment. The November 2017 General Election was effectively administered without any reported voting equipment issues. The transition to paper-based voting systems on a truncated timeline was incredibly successful and significantly increased the security of the election.

None of this would have been possible without the great work of our local election officials, who struggle with a consistent lack of financial resources; my Deputy Commissioner, Liz Howard; my CIO, Matt Davis; VITA, especially Mike Watson; and so many others, including Tracy Howard, Former President, VRAV; Katie Boyle, Virginia Association of Counties Director of Government Affairs; Verified Voting; and last but certainly not least, the EAC. In essence, the decertifications have gone smoothly because of the teamwork between state and local officials, national organizations, state organizations, voting equipment vendors and the veritable army of officers of election who assist with administering our elections with little or no pay every year.

Although it's clearly possible to transition quickly, doing so is less than ideal. As the voting equipment issue is far from resolved, I request that you consider the following recommendations which, I believe, will make these issues much easier to manage in the future:

1) Funding elections is a shared responsibility at the local, state, and federal level. Congress needs to ensure sufficient federal funding is available for states to procure and maintain secure voting equipment and increase security of all election systems. This is a critical need.

2) The EAC has been critical to ensuring that a baseline set of standards for voting systems, adequate testing protocols, and certified test labs are available to states and Congress should retain and fully fund this exceptionally important resource to states.

3) In order to ensure the use of secure voting equipment in the future, Congress should require federal certification of all voting systems used in federal elections. This federal certification protocol would ensure a security baseline – and allow for states to require additional and state-specific testing. In addition, it would address the need for ongoing and periodic testing without subjecting the vendors to 50 different periodic testing schedules, and mandate that the vendors provide equipment for testing upon request. Federal certification also should be required for electronic pollbooks, which currently are not subject to any federal guidelines. If mandatory federal certification is not a realistic solution, then, at minimum, Congress should empower and fund the EAC to expand its current voluntary voting equipment guidelines to include guidelines applicable to electronic pollbooks and incorporate periodic security testing as a prerequisite to maintain certification.

4) Congress should establish an accreditation system for election administrator training to ensure that the individuals responsible for this most fundamental American right are equipped with the appropriate skill and knowledge set.

Thank you again for inviting me to join you today and your interest in hearing from election administrators about the work being done to secure the nation's voting systems. We look forward to continuing to work with Congress to ensure sufficient federal resources are available to state and local election officials to continue this important work.

Mr. HURD. Thank you, sir.

Dr. Blaze, great to have you here. And having participated and walked through the voting village at DEFCON, I saw up close and personal what the white hat hacker community and security research community does and the impact they have on public policy. And so thank you for your efforts there, and you're now recognized for 4 minutes.

STATEMENT OF MATTHEW BLAZE, PH.D.

Mr. BLAZE. Thank you very much, Mr. Chairman, the ranking members, and all of the members who are here today.

As a computer scientist who specializes in the security of large scale critical systems, I've had an interest in electronic voting technology since it was first introduced at large scale in the United States after the passage of the Help America Vote Act in 2002.

In particular, I lead several of the teams commissioned in 2007 by the secretaries of state of California and Ohio to evaluate the voting system products used in those States, as well as elsewhere in the Nation. I also helped organize the DEFCON voting machine hacking village that was held this summer, at which these systems were made available really to a larger community for the first time—for the first time ever.

Virtually every aspect of our election process, from voter registration to ballot creation to casting ballots, and then to counting and reporting election results is, today, controlled in some way by software. And, unfortunately, software is notoriously difficult to secure, especially in large scale systems such as those used in voting.

And the software used in elections is really no exception to this. It's difficult to overstate how vulnerable our voting infrastructure that's in use in many States today is, particularly the compromise by a determined and well-funded adversary. For example, in 2007, our teams discovered exploitable vulnerabilities in virtually every voting system component that we examined, including back-end election management software as well as, particularly, DRE voting terminals themselves.

At this year's DEFCON event, we saw that many of the weaknesses discovered in 2007, and known since then, not only are still present in these systems, but can be exploited quickly and easily by nonspecialists who lack access to proprietary information such as source code. These vulnerabilities are serious, but ultimately unsurprising.

The design of DRE systems makes them particularly dependent on the really Herculean task of securing all of the software components that they depend on. And this would be, under the best of circumstances, an extraordinarily difficult thing to do. So what we're seeing is both alarming as well as unsurprising.

Worst, as we saw in 2016, we largely underestimated the nature of the threat to the extent these systems are intended even to be secure. That is, they're designed against a traditional adversary who wants to cheat in an election and alter the results. But there's actually an even more serious adversary, a nation state or a state actor who might seek to disrupt an election, cast doubt on the legitimacy of the outcome, and cause a threat to our confidence in legitimacy of our elected officials.

I discuss all of these issues in detail in my written testimony, and I offer really three particular recommendations. The first is that paperless DRE voting machines should be immediately phased out from U.S. elections, in favor of systems such as precinct counted optical scan ballots that leave a direct artifact of the voters' choices.

Secondly, statistical risk limiting audits should be used after every election to enable us to detect software failures in the backend systems and recover the true election results if a problem is found.

And then, finally, additional resources, infrastructure, and training should be made available to State and local voting officials to help them more effectively defend their systems against increasingly sophisticated adversaries.

So thank you very much.

[Prepared statement of Mr. Blaze follows:]

MATT BLAZE

UNIVERSITY OF PENNSYLVANIA[1]

US HOUSE OF REPRESENTATIVES
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
SUBCOMMITTEE ON INFORMATION TECHNOLOGY AND
SUBCOMMITTEE ON INTERGOVERNMENTAL AFFAIRS
HEARING ON CYBERSECURITY OF VOTING MACHINES

NOVEMBER 29, 2017

[1] University of Pennsylvania Computer and Information Science, 3330 Walnut Street, Philadelphia, PA 19104. *mab@crypto.com*. Affiliation for identification only.

INTRODUCTION

Thank you for the opportunity to offer testimony on the important questions raised by the security of the technology used for elections in the United States.

For the last 25 years, my research and scholarship has focused on the security of cryptographic, computing and communications systems, especially as we rely on insecure platforms such as the Internet for increasingly critical applications. My work has focused particularly on the intersection of this technology with public policy issues. For example, in 2007, I led several of the teams that evaluated the security of computerized election systems from several vendors on behalf of the states of California and Ohio.

I am currently an associate professor in the computer and information science department at the University of Pennsylvania, where I direct the Distributed Systems Laboratory. From 1992 to 2004, I was a research scientist at AT&T Bell Laboratories. This testimony is not offered on behalf of any organization or agency.

In this testimony, I will give an overview of the security issues facing elections in the United States today, with emphasis on the risks and vulnerabilities inherent in Direct Recording Electronic (DRE "touchscreen") voting machines as well as the exposure of our election infrastructure to disruption by national security adversaries.

I offer three specific recommendations:

- Paperless DRE voting machines should be immediately phased out from US elections in favor of systems, such as precinct-counted optical scan ballots, that leave a direct artifact of the voter's choice.
- Statistical "risk limiting audits" should be used after *every* election to detect software failures and attacks.
- Additional resources, infrastructure, and training should be made available to state and local voting officials to help them more effectively defend their systems against increasingly sophisticated adversaries.

I. ELECTIONS AND SOFTWARE SECURITY

A consequence of our federalist system is that US elections are in practice highly decentralized, with each state responsible for setting its own standards and procedures for registering voters, casting ballots, and counting votes. The federal government sets broad standards for such issues as accessibility, but it is largely uninvolved in day-to-day election operations. In most states, election management functions are largely delegated to local county and town governments, which are responsible for registering voters, procuring voting equipment, creating ballots, setting up and managing local polling places, counting votes, and reporting the results of each contest. Thousands of individual local election offices thus manage and secure the voting process for most of the American electorate.

Elections in the US are among the most operationally and logistically complex in the world. Many jurisdictions have large numbers of geographically dispersed voters, and most elections involve multiple ballot contests and referenda. The requirements for protection against potentially very sophisticated adversaries, ballot secrecy, fair access to the polls, and rapid, accurate reporting of results make secure election management one of the most formidable – and potentially fragile – information technology problems in government.

Computers and software play central roles in almost every aspect of our election process: managing voter registration records, defining ballots, provisioning voting machines, tallying and reporting results, and controlling electronic voting machines used at polling places.[2] The integrity and security of our elections are thus inexorably tied to the integrity and security of the computers and software that we rely on for these many functions.

The passage of the Help America Vote Act (HAVA) in 2002 accelerated the computerization of voting systems, particularly with respect to the ways in which voters cast their ballots at local polling stations. HAVA provided funds for states to replace precinct voting equipment with "accessible" technology. Unfortunately, as implemented, some of this technology has had the unintended consequence of increasing the risk of elections being exposed to compromise by malicious actors.

[2] Today, the "back office" of a typical election administration office is much like that of any modern business, with local computer networks tying together desktop computers, printers, servers, and Internet access. This increasing connectivity served as a critical avenue for what US intelligence agencies identified as Russian military intelligence actors.

A. Election Software and Hardware

A typical[3] county election office today depends on computerized systems and software for virtually every aspect of registering voters and conducting elections. Generally, an election office workflow will include at least the following pre- and post- election functions:

Voter registration – The ongoing maintenance of an authoritative database of registered voters in the jurisdiction, including the precinct-by-precinct "poll books" of voters (which might be on paper or in electronic form) that are used to check in voters at precinct polling stations.

Ballot definition – The pre-election process of creating data files that list the various contests, candidates, and rules (e.g., number of permitted choices per race) that will appear on the ballot. The ballot definition is used to print paper ballots, to define what is displayed on touchscreen voting terminals, and to control the vote tallying and reporting software. Local races (such as school boards) may sometimes require that different ballot definitions be created for different precincts within a county in any given election.

Voting machine provisioning – The pre-election process of configuring the individual precinct voting machines for an election. This typically includes resetting internal memory and loading the appropriate ballot definition for each precinct. Depending on the model of voting machine, provisioning typically involves using a computer to write removable memory cards that are installed in each machine.

Absentee and early ballot processing – The process of reading and tabulating ballots received by mail and from early voting polling places. Mail votes are typically processed in bulk by high-volume optical scan ballot reading equipment.

Tallying and reporting – The post-election process of tabulating the results for each race received from each precinct and reporting the overall election outcomes. This process typically involves using a computer to read memory card media retrieved from precinct voting machines.

[3] The precise nature of the systems used and how they interact with one another will vary somewhat depending on the vendors from which the systems were purchased and the practices of the local jurisdiction.

Each of the above "back end" functions employs specialized software running on computers. Depending on the size and practices of the county, the same computers may be used for more than one function (e.g., the ballot definition computer might also serve as the tallying and reporting computer). These computers are typically off-the-shelf desktop machines running a standard operating system (such as Microsoft Windows), equipped with electronic mail and web browser software along with specialized voting software. Election office computers are typically connected to one another via a wired or wireless local area network, which may have a direct or indirect connection (sometimes via a firewall) to the Internet.

In some jurisdictions, some of the various back end functions (most often those concerned with voter registration databases and ballot definition), may be outsourced by a county or state to an election service contractor. These contractors provide specialized assistance with such as creating ballots in the correct format, managing voter registration databases, creating precinct poll books, and maintaining voting machines. Not all jurisdictions employ contractors, however.

Voting equipment used at precincts is computerized as well, although generally packaged in specialized hardware rather than off-the-shelf equipment. This equipment includes:

Direct Recording Electronic (DRE) Voting Machines – DRE machines are special-purpose computers that display ballot choices to the voter (based on the ballot definition) and record voter choices. Both the ballot definition configuration and the vote count are typically stored on removable memory media.[4]

Optical Scan Ballot Readers – Optical scan ballot readers are specialized computers that read voter-marked paper ballots. The ballot is read according to the ballot definition configuration (typically on removable memory media), and a tally is maintained in memory (also typically on removable media). The machine also captures the scanned ballots and stores them in a mechanically secured ballot box.

Ballot Marking Devices – Ballot marking devices are an assistive

[4] Some models of DRE machines can be equipped with a *Voter Verified Paper Audit Trail (VVPAT)* option in which the voters' selections are printed on a paper tape roll that is visible to the voter. VVPATs can assist with determining the voter's intent during a recount, but their efficacy depends on each voter's diligence in confirming that their choices are correctly recorded on the paper tape before they leave the voting booth.

technology used in optical scan systems to allow visually or mobility impaired voters to create ballots for subsequent scanning. They are similar to DRE machines in that they display (or read aloud) the ballot electronically, based on a ballot definition configuration, and accept voter choices for each race. However, instead of recording the choices in memory, they print a marked paper ballot that can then be submitted through an optical scan ballot reader.

Electronic Poll Books – These devices are typically tablet-style computers that contain an authoritative copy of the database of registered voters at each precinct. Electronic poll books are not used directly by voters, but rather by precinct poll workers as voters are checked in at their polling place. They are not used in all jurisdictions.

B. Software and Election Security

Complex software systems are notoriously difficult to secure, and those that perform the various functions described above are no exception.[5] There are several avenues of vulnerability in such systems. Common software "bugs" often introduce vulnerabilities that can be exploited by an adversary to silently compromise the integrity of data or make unauthorized (and difficult to detect) changes to the behavior of systems. Configuration and system management errors (such as the use of vulnerable out-of-date platforms and weak passwords) can further compromise security. Computer networks (which are not generally used by precinct voting machines themselves but are commonly connected to back end systems in election offices) compound these risks by introducing the possibility of remote attack over the Internet.

The integrity of the vote today largely depends on the integrity of the software systems – running on voting machines and on county election office networks – over which elections are conducted. Any security weakness in any component of any of these systems can serve as a "weak link" that can allow a malicious actor to disrupt election operations, alter tally results, or disenfranchise voters.

[5] The fact that software systems can be, and often are, insecure and vulnerable to attack is not unique to election systems, of course. Serious data breaches are literally daily events across the public and private sectors, and cybersecurity is widely recognized to be a serious national security problem. To the extent that elections depend on software or are administered by networked computing systems, they are subject to all the same risks.

In many electronic voting systems in use today, a successful attack that exploits a software flaw might leave behind little or no forensic evidence. This can make it effectively impossible to determine the true outcome of an election or even that a compromise has occurred.

Unfortunately, these risks are not merely hypothetical or speculative. Many of the software and hardware technologies that support US elections today have been shown to suffer from serious and easily exploitable security vulnerabilities that could be used by an adversary to alter vote tallies or cast doubt on the integrity of election results.

II. DRE ELECTRONIC VOTING SYSTEMS HAVE PROVEN VULNERABLE TO A RANGE OF KNOWN, EXPLOITABLE SECURITY FLAWS

Security concerns about computerized voting systems have been raised from the moment such systems were first proposed. Most of these concerns have focused on electronic voting equipment used at polling stations, although the "back end" software used to manage voter registration, provision voting machines, and tally are also critical to the integrity of the vote.

From a security perspective, the most problematic and risky class of electronic voting systems are those that employ *Direct Recording-Electronic (DRE)* machines. DRE machines are special purpose computers programmed to present the ballot to the voter and record the voter's choices on an internal digital medium such as a memory card. At the end of the election day, the memory card containing the vote tallies for each race is generally removed or electronically read from the machine and delivered to the county election office, where the tallies from each precinct are recorded by the county tallying software. DRE machines are sometimes informally called "touchscreen" voting machines, although not all DRE models use actual touchscreen displays (nor are all voting devices that employ touchscreens DREs).

The design of DREs makes them inherently difficult to secure and yet also makes it especially imperative that they *be* secure. This is because the accuracy and integrity of the recorded vote tally depends completely on the correctness and security of the machine's hardware, software, and data. Every aspect of a DRE's behavior, from the ballot displayed to the voter to the recording and reporting of votes, is under control of the DRE hardware and software. Any security vulnerability in this hardware or software, or any ability for an attacker to alter (or re-load new and maliciously behaving) software running on the machine, not only has the potential to alter the vote tally, but can make it impossible to conduct a meaningful recount (or even to detect that an attack has occurred) after the fact.

DRE-based systems introduce several avenues for attack that are generally not present (or as security-critical) in other voting technologies. Successful exploitation of any *one* of these attack vectors can compromise elections in ways from which it may not be possible to recover:

- Alteration or deletion of vote tallies stored in internal memory or removable media

- Alteration or deletion of ballot definition parameters displayed to voters [6]
- Alteration or deletion of electronic log files used for post-election audits and detecting unauthorized tampering

These attacks might be carried out in any of several ways, each of which must be reliably defended against by the DRE hardware and software:

- Direct tampering with data files stored on memory cards or accessible through external interface ports
- Unauthorized replacement of the certified software running on the machine with a maliciously altered version
- Exploitation of a pre-existing vulnerability in the certified software

Successfully exploiting just *one* of these avenues of attack can be sufficient to undetectably compromise an election. The design of DREs makes it necessary not only that the hardware be highly secure against unauthorized tampering, but that the certified software running on them not suffer from *any* vulnerabilities that could be exploited by a malicious actor. This makes the security requirements for DREs more stringent – and more easily defeated – than for almost any other current election technology.

Unfortunately, the DRE-based systems purchased by and used in various states under HAVA have repeatedly been found to suffer from exactly these kinds of exploitable hardware and software vulnerabilities

A. The 2007 California and Ohio Studies

To date, the most extensive independent studies of the security of electronic voting systems were commissioned ten years ago by the Secretaries of State of California and Ohio. Expert review teams were

[6] An incorrect (or maliciously altered) DRE ballot definition can make it impossible to determine the true election results even without any malicious software exploitation. For example, in York County, PA, a DRE ballot definition programming error in the 2017 general election appears to have allowed candidates in some local races to be voted for twice, with the possible consequence that the election will have to be invalidated and redone. See http://www.ydr.com/story/news/2017/11/08/voting-machine-problems-what-york-countys-options/843423001/ . Paper-based systems, in contrast, are more robust against such errors. For example, the 2000 general election in Bernalillo County, NM had a similar error in their punch card counting software, but was later able to correct the error without a new election; see https://www.wsj.com/articles/SB976838091124686673

given access to the voting machine hardware and software source code of every system certified for use in those states. The systems used in California and Ohio were also certified for use in most of the rest of the country, so these studies effectively covered a large fraction of available electronic voting equipment and software. I led the teams that reviewed the Sequoia products (for the state of California) and the ES&S products (for the state of Ohio); other teams in these studies reviewed the Diebold/Premier and Hart InterCivic products.[7]

In both studies, every team found and reported serious exploitable vulnerabilities in *almost every component* examined. In most cases, these vulnerabilities could be exploited by a single individual, who would need no more access than an ordinary poll worker or voter. Such an attacker would be able to alter vote tallies, load malicious software, or erase audit logs. Some of the vulnerabilities found were the consequence of software bugs, while others were caused by fundamental architectural properties of the system architecture and design. In some cases, compromise of a single system component (such as a precinct voting machine) was sufficient to compromise not just the vote tally on that machine, but to compromise the entire county back end system.

In response, California and Ohio ordered some equipment decertified and some election-day procedures modified. However, all the vulnerable equipment and software remained certified for use in at least some other states.

Some equipment vendors and local voting officials claimed at the time that the findings of the California and Ohio studies were irrelevant or overstated, that any problems identified could be easily fixed, and that it would be difficult or impossible for anyone but an expert with extensive experience and access to privileged information (such as source code) to exploit vulnerabilities in practice. However, as exercises such as the DEFCON Voting Village (described below) have demonstrated, not only do these systems remain vulnerable, but they can be readily exploited by people with no more than ordinary computer science experience and expertise and without access to any secret or proprietary information.

[7] The various final reports of the California "Top-To-Bottom Review" studies can be found at http://www.sos.ca.gov/elections/voting-systems/oversight/top-bottom-review/ . The final report of the Ohio "Project EVEREST" study can be found at https://www.eac.gov/assets/1/28/EVEREST.pdf

B. The 2017 DEFCON Voting Machine Village Exercise

The DEFCON conference is one of the world's largest and best-known computer security "hacker" conferences. This year's DEFCON was held July 27-30, 2017 in Las Vegas, NV, and drew approximately 25,000 participants from around the world. DEFCON participants have broad interest in technology, and include security researchers from industry, government, and academia, as well as individual hobbyists.

This year, for the first time, DEFCON featured a *Voting Machine Hacking Village* ("Voting Village") to give participants an opportunity to examine and get hands-on experience with the security technology used in US elections, including voting machines, voter registration databases, and election office networks. I was one of the organizers of the Voting Village.[8]

The voting machines available in the Voting Village were chiefly DRE models. We acquired (from the surplus market) and made available to participants a sampling of 25 pieces of election hardware, including voting machines and "electronic poll books" used by precinct workers to verify and check in voters at polling places. All but one model of machine in the Voting Village is still certified for use in U.S. elections in at least one jurisdiction today. The Voting Village also featured a mock back-office training "range" to simulate back-end databases and networks of county election administrators.

The DEFCON Voting Village was not intended to be a formal security assessment or test, but rather an opportunity for a general audience of technologists to examine election equipment and systems. However, participants were encouraged to critically examine and probe the equipment and software for vulnerabilities, and to seek practical ways to compromise security mechanisms. No proprietary information, computer source code, or specialized tools were made available.

The results of the Voting Village were summarized in detail in a report.[9] It is notable that participants, who did not have any previous special expertise in voting machines or access to any proprietary information or source code, were very quickly able to find ways to compromise *every* piece of equipment in the Village by the end of the weekend. Depending on the

[8] Organizers of the DEFCON Voting Village included the author as well as Jake Braun, Hari Hursti, Joseph Lorenzo Hall, Margaret MacAlpine, and Jeff Moss.

[9] The final report is available for download at: https://www.defcon.org/images/defcon-25/DEF%20CON%2025%20voting%20village%20report.pdf

individual model of machine, participants found ways to load malicious software, gain access to administrator passwords, compromise recorded votes and audit logs, or cause equipment to fail. In most cases, these attacks could be carried out from the ordinary interfaces that are exposed to voters and precinct poll workers. The first machine was compromised by a participant within 90 minutes of the doors opening.

The ease with which participants compromised equipment in the Voting Village should be regarded as both alarming and yet also unsurprising. It is alarming because the very same equipment is in use in polling places around the United States, relied on for the integrity of real elections. But it is also ultimately unsurprising. Versions of every machine at DEFCON had been examined in the 2007 studies and found to suffer from basic, exploitable security vulnerabilities. It should not come as any surprise that, given access and motivation, people of ordinary skill in computer security would be able to replicate these results. It is, in fact, exactly what previous studies of these machines warned would happen.

In summary, the DEFCON Voting Village demonstrated that much of the DRE voting technology used in the US is vulnerable not just to hypothetical expert attack in a laboratory environment, but also to practical exploitation in the field by non-specialists.

III. CURRENT ELECTRONIC VOTING SYSTEMS HAVE NOT BEEN ENGINEERED TO RESIST NATION-STATE ADVERSARIES

The traditional "threat model" against which electronic voting systems have been evaluated has been focused on resisting traditional election *fraud*, in which criminal conspirators, perhaps assisted by corrupt poll workers or election officials, attempt to "rig" an election to favor a preferred candidate in a local, state, or national contest. Fraud might be accomplished by altering votes, adding favorable votes, deleting unfavorable votes, or otherwise compromising the security mechanisms that protect the ballot and tally.

While virtually every study of electronic voting technology has raised questions about the ability of current systems to resist serious efforts at fraud, traditional election fraud is not the only kind of threat, or even the most serious practical threat, that a voting systems must resist today.

Electronic voting systems must resist not only fraud from corrupt candidates and supporters, but also election *disruption* from hostile nation-state adversaries. This is a much more formidable threat, and one that current systems, especially those using DRE technology, are even less equipped to resist.

The most obvious difference between traditional fraud from corrupt candidates and disruption by hostile state actors is the expected resources and capabilities available to the attacker. The intelligence services of even relatively small nations can marshal far greater financial, technical, and operational resources than even the most sophisticated corrupt domestic criminal attacker. For example, intelligence services can be expected to conduct espionage operations against the voting system *supply chain*. In such operations, the aim might be to obtain confidential source code or to secure surreptitious access to equipment before it is even shipped to county officials. Hostile intelligence services can exploit information and other assets developed broadly over extended periods of time, often starting well before any specific operation or attack has been planned.

But their greater resources are not the most important way that hostile state actors can be a more formidable threat than corrupt candidates or poll workers. They also have easier goals. The aim of traditional "retail" election fraud is to tilt the outcome in favor of a particular candidate. That is, to succeed, the attacker must generally alter the reported vote count or add, change, or delete votes. But a hostile state actor – via an intelligence service such as Russia's GRU – might be satisfied with merely *disrupting* an election or calling into question the *legitimacy* of the official outcome. With election systems so heavily dependent on demonstrably insecure software voting equipment, this kind of disruption could be comparatively simple to accomplish, even at a national scale.

A hostile state actor who can compromise even a handful of county networks might not need to alter any actual votes to create widespread uncertainty about an election outcome's legitimacy. It may be sufficient to simply plant suspicious (and detectable) malicious software on a few voting machines or election management computers, create some suspicious audit logs, delete registered voters from the rolls, or add some obviously spurious names to the voter rolls. If the preferred candidate wins, they can simply do nothing (or, ideally, use their previously arranged access to restore the compromised networks to their original states, erasing any evidence of compromise). If the "wrong" candidate wins, however, they could covertly reveal evidence that county election systems had been compromised, creating public doubt about whether the election had been "rigged". This could easily impair the ability of the true winner to effectively govern, at least for a period of time.

Electronic voting machines and vote tallies are not the only potential targets for such attacks. Of particular concern are the back end systems that manage voter registration, ballot definition, and other election management tasks. Compromising any of these systems (which are often connected, directly or indirectly, to the Internet and therefore potentially remotely accessible) can be sufficient to disrupt an election while the polls are open or cast doubt on the legitimacy of the reported result. The decentralization of election operations, managed by thousands of individual local offices throughout the nation (with widely varying resources) is sometimes cited as a strength of our electoral process. However, this decentralization can be turned to the adversary's advantage. An attacker can choose arbitrarily from among whatever counties have the weakest systems – those with the least secure software or most poorly defended networks and procedures – to target.

It is beyond the scope of my testimony to speculate on specific intrusions that occurred against state and local election management systems in the 2016 US general election, much of which remain under investigation. It has been reported that voter registration management systems in at least several states were targeted for exploitation and access. It is unclear whether voting machines or tallying systems were also targeted. However, targeting and exploiting such systems would have been well within the capability of any major rival intelligence service.

In summary, the architecture of current electronic voting systems, especially those based on DRE voting machines, makes disruption attacks especially attractive to adversaries and difficult to effectively prevent. These systems can give hostile state actors interested in disruption an even *easier* task than that facing corrupt candidates seeking to steal even a small local office. And the consequences of election disruption strike at the very heart of our national democracy.

IV. Recommendations: US Elections Should Employ Paper Ballots and Risk-Limiting Audits

It is perhaps tempting to conclude pessimistically that election technology in the US is fatally flawed, leaving our nation irreparably vulnerable to election fraud and foreign meddling. But while it is true that the current situation exposes us to significant risk, it is by no means hopeless or beyond repair. Relatively simple, and available, technologies can be deployed that render our elections significantly more robust against attack.

While DRE voting machines suffer demonstrably fundamental weaknesses, other electronic voting technologies are significantly more resilient in the face of compromise. The most important feature required is that there be a reliable record of each voter's true ballot selections that can be used as the basis for a recount if the software systems fail or are called into question.

Among currently available, HAVA-compliant voting technologies, the state of the art in this regard are *precinct-counted optical scan* systems. In such systems, the voter fills out a machine-readable paper ballot form (possibly with the aid of an assistive ballot marking device for language-, visually- and mobility-impaired voters), which is deposited into a ballot scanning device that reads the ballot choices, maintains an electronic tally, and retains and secures the marked paper ballots for subsequent audit. After the polls close, the electronic tally records are read from each ballot scanner and the election results calculated.

The paper records of votes that precinct-counted optical-scan systems provide are a necessary, but not by themselves sufficient, safeguard against software compromise in a computerized election system. Non-DRE systems can still suffer from flaws and exploitable vulnerabilities in voting machine and back end software. The second essential safeguard is a reliable process for detecting whether the software is reporting incorrect results, and to recover the true results if so.

The most reliable and well-understood method to achieve this is through an approach called *risk-limiting audits*.[10] In a risk limiting audit, a statistically significant randomized sample of precincts have their paper

[10] A good introduction to the theory and practice of risk limiting audits in elections can be found at https://www.stat.berkeley.edu/~stark/Preprints/RLAwhitepaper12.pdf .

ballots manually counted by hand and the results compared with the electronic tally. (This must be done for *every* contest, not just those with close results that might otherwise call into question the outcome.) If discrepancies are discovered between the manual and electronic tallies, additional manual counts are conducted. The effect of risk-limiting audits is not to eliminate software vulnerabilities, but to ensure that the integrity of the election outcome does not depend on the herculean task of securing every software component in the system. This important property is called *strong software independence.*[11]

Optical scan paper ballots and risk-limiting audits comprise a critical, and readily deployable, safeguard against both traditional election fraud and nation-state disruption. Taken together, they permit us to more safely enjoy the benefits of computerized election management, without introducing significant new costs or requiring the development of speculative new technology. The technology required for is available *today*, from multiple vendors, and is already in use in many states.

As important as paper ballots and risk-limiting audits are, however, they are not panaceas that solve every threat to our elections. It is also critical that the state and county backend computer networks and systems used for election management and voter registration be vigilantly protected against compromise. As we saw in 2016, hostile adversaries might attempt to breach not just voting machines, but also backend election management systems and voter registration database systems, which are often connected, directly or indirectly, to the Internet.

It is no exaggeration to observe that state and local election officials serve on the front lines of our national cybersecurity defense. They must be given sufficient resources, infrastructure, and training to help them effectively defend their systems against an increasingly sophisticated – and increasingly aggressive – threat environment. It is notable that the budgets for election administration often must compete for resources with essential local services such as fire protection and road maintenance. Election management represents only a miniscule fraction of the total national spending on political campaigns. Additional investment here will pay significant dividends for our security.

Simply put, much of our election infrastructure remains vulnerable

[11] See Ron Rivest. "On the notion of 'software independence' in voting systems". *Phil. Trans Royal Society A*. Volume 366 Issue 1881. October 28, 2008. http://rsta.royalsocietypublishing.org/content/366/1881/3759 .

to practical attack, with threats that range from traditional election tampering in local races to large-scale disruption by national adversaries. We should take no comfort if such attacks have not yet been widely detected. At best, it is only because, for whatever reason, serious attempts have not yet been made. It is only a matter of time before they will.

Safeguards such as those described above serve our democracy in critically important ways. They provide a significant improvement to election security, both in our ability to resist attack and in our ability to recover from attack should one occur. Perhaps most importantly, they provide meaningful assurance to voters that their votes truly count and that their elected officials are governing truly legitimately. Our republic cannot for long survive without the confidence that comes from that assurance.

Mr. HURD. Thank you, sir.

Ms. Hennessey, you're now recognized for 4 minutes.

STATEMENT OF SUSAN HENNESSEY

Ms. HENNESSEY. Thank you to Chairman Hurd, Ranking Member Kelly, to Chairman Palmer, and Ranking Member Butler Demings, and to the distinguished members for the opportunity to speak to you today.

My name is Susan Hennessey. I am the executive editor of Lawfare and a fellow at the Brookings Institution where my research focuses on the law and policy governing cybersecurity and surveillance. Prior to Brookings, I served as an attorney for the National Security Agency, though my comments today reflect only my personal views, and not those of my current or prior employer.

I'd like to begin by noting how extraordinary it is that a full year after the last presidential election, there is still enduring attention to the issue of election security. This moment really represents a remarkable opportunity to take long overdue steps towards securing Federal and State elections. In order to do so, however, it is necessary to carefully define the issues and to disentangle pure election security from broader information operations, or covert influence campaigns.

Information operations certainly impacts the broader context in which elections occur, but they are distinct problems with distinct solutions.

The matter currently before these committees is narrower, but no less pernicious: the threat to election infrastructure and voting systems related to the management and administration of elections. The election security threat is not limited exclusively to changing the vote counts. As other experts have testified here today, altering vote tallies is technically possible. However, it remains difficult to do so on the scale necessary to predictably change the outcome of the statewide or national election.

The probable actors with both the incentives and technical capacity to carry out sophisticated attacks are foreign governments, which would need to avoid both forensic detection and that of the U.S. and allied intelligence communities. Unfortunately, U.S. adversaries have a far more achievable aim, to undermine the confidence of the American people in their government and their processes and institutions, and in the selection of their leaders. To do so, a malicious actor needs only to penetrate systems in a manner that introduces uncertainty. This landscape increases the importance of being cautious in how we discuss election security issues to avoid inadvertently undermining confidence ourselves.

Congressionally driven solutions should account for international and domestic realities. Internationally, while most recent attention has been on Russia, any number of U.S. adversaries, including China, North Korea, and Iran, possess the capabilities and interest to be of genuine concern. Enduring solutions cannot be country-specific.

Domestically, a strong tradition of Federalism and election administration ensures that despite clear constitutional authority, any perceived Federal overreach will meet strong resistance from States on political and policy grounds. Keeping those features and the nature of the threat in mind, I believe Congress should adopt the following broad solutions which are detailed more extensively in my statement for the record.

First, to direct the development of a national strategy for securing elections aimed at protecting systems, deterring bad actors and bolstering public confidence. Second, provide Federal resources to States in the form of funding, support, and best practices. Third, regulate election technology vendors, which currently operate in limited and proprietary markets that leave States with insufficient power to dictate security standards. Fourth, lead the development of international norms against election interference.

Finally, Congress, as our primary elective body, must renew and sustain political commitment to the issue of election security, and reestablish norms that have been broken in the way we discuss election integrity and outcomes.

Thank you, again, for the opportunity to address you today. I look forward to taking questions on this important national security issue.

[Prepared statement of Ms. Hennessey follows:]

November 29, 2017

Susan Hennessey,
Written Statement for the House Committee on Oversight and Government Reform:
Subcommittees on Information Technology and Intergovernmental Affairs

Cybersecurity of Voting Machines

Thank you to Chairman Hurd and Ranking Member Kelly, to Chairman Palmer and Ranking Member Butler Demings, and to the distinguished members for the opportunity to speak to you today.

My name is Susan Hennessey and I am Fellow of National Security Law in Governance Studies at the Brookings Institution and the Executive Editor of Lawfare. My research at Brookings focuses in particular on the law and policy governing cybersecurity and surveillance. Prior to joining Brookings, I served as an attorney in the Office of General Counsel for the National Security Agency from 2013 to 2015. My comments here today reflect only my personal views and not those of my current or prior employer.

I want to begin by noting the extraordinary fact that a full year after the last presidential election, there is still enduring attention—among the public, in academia, in the executive branch, and on Capitol Hill—to the issue of election security. This moment presents a remarkable opportunity to take long-overdue steps toward securing federal and state elections.

Today, I hope to map some of the current landscape, both with respect to the nature of the foreign threat, domestic considerations, and possible solutions. Broadly, I want to suggest that Congress work in concert with the executive branch to:

- *Develop a national strategy for securing elections.*
- *Provide federal resources in the form of funding, support, and best practices.*
- *Regulate election-technology vendors.*
- *Lead the development of international norms against election interference.*
- *Renew and sustain political commitment to the issue of election security.*

Before turning to those recommendations, however, it may be useful to review some necessary background.

Defining the "Election Security" Threat

First, how should we understand the election-security threat? As demonstrated by the 2016 U.S. presidential election, the pertinent security issues are immensely complex and wide-ranging. In order to develop a sensible framework, we must disentangle pure election-security issues from broader information operations or covert influence campaigns.

Information operations certainly impact the broader context in which elections occur—including the process of public debate and decision-making as we exercise the fundamental democratic choice. The threat of disinformation campaigns in elections is extremely high, it has materialized in the past, and it will persist in the future. However, for this committee's purposes, that issue should be viewed as a distinct challenge with its own set of available solutions, some of which may come into tension with core American values such as freedom of speech.

The matter currently before this body is more easily defined, though no less difficult and pernicious: the threat to election infrastructure and "voting systems" related to the management and administration of elections. Election infrastructure should be understood to include voter-registration systems, voter check-in systems (also known as poll books), voting terminals, central tabulation and election-night reporting systems, as well as post-election auditing systems. A more difficult question is which, if any, systems used by campaigns, parties, and candidates should also be considered part of election infrastructure.

Understanding the Nature of the Threat

Other experts before the committee today will discuss the technical threats to voting machines and systems. I believe, in context, a fair layperson characterization of that threat is to say that actually changing vote tallies is not a technical impossibility, but it is extremely difficult to do so on the scale necessary to predictably change the outcome of a statewide or national election. The most probable actors with both the incentives and technical capacity to carry out sophisticated attacks are foreign governments, which would need to evade not only forensic detection, but also detection by the United States and allied intelligence communities in order to be successful. As we've seen following the 2016 election, that is an exceptionally difficult task.

Unfortunately, U.S. foreign adversaries' intentions are not merely to change outcomes, but rather a more achievable aim: to undermine confidence. If our adversaries can successfully shake the confidence of the American people in their government, in their processes and institutions, and in the selection of their leaders, then that is a successful assault on liberal democracy. That is far easier to achieve than predictably changing election outcomes. To do so, a malicious actor needs only to penetrate systems such that experts and election officials can no longer express sufficient certainty in the integrity of a system or result.

The timeline of the 2016 U.S. election interference and response demonstrates the importance of public confidence in voting systems. The prior administration did not publicly comment on or confirm early reports of Russian attempts to influence the U.S. election. Despite detailed public accounts as early as June 2016, the administration waited until October 2016 to issue its first formal attribution. The administration released its statement only after media reports that election systems in up to twenty-one states had been targeted and the statement had the clear purpose of reassuring the American public that voting systems remained secure.[1] This is a good illustration of how such activity—in this case described as the "scanning and probing of [state] election-related systems" but not successful penetrations—can force the government to respond publicly, even where it does not suspect impactful interference has occurred.

Other methods to undermine confidence might include disrupting the election process through denial-of-service attacks, interfering with voter registration, manipulating voting interfaces to generate bias, or compromising audit trails.

Information operations may similarly target public confidence in elections. Indeed, many of the information operations that occurred in 2015 and 2016 were aimed at creating the social conditions in which delegitimizing U.S. election results might be most fruitful. The Intelligence Community Assessment of Russian Activities and Intentions in Recent U.S. Elections notes that Russian social media bots had prepared a #DemocracyRIP hashtag campaign to call into question the legitimacy of the election had it been decided for Secretary Clinton instead of President Trump.[2] While it is important to acknowledge the interactions between the two, it remains useful to distinguish to the extent possible information operations like these from election-security issues.

If the goal of threats to election infrastructure is to undermine confidence, rather than to change outcomes, the importance of careful messaging becomes clear. The manner in which we discuss vulnerabilities to election systems could inadvertently achieve our adversaries' goals. If the American people receive the message that voting systems are not secure and cannot be secured, or that there is reason to question the reliability of

[1] "Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security." *Department of Homeland Security,* Oct. 7, 2016. https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national

[2] "Assessing Russian Activities and Intentions in Recent US Elections." *Office of the Director of National Intelligence* at 12, Jan. 6, 2017. https://www.dni.gov/files/documents/ICA_2017_01.pdf

election results, that risks undermining confidence in the electoral system. The appropriate response is not to ignore the existence of genuine problems, but instead to exercise caution in public messaging.

Surveying Recent Threats

It is important to note the range of objectives and actors in the space. The lion's share of attention over the past year has been on Russia, but any number of U.S. adversaries, including China, North Korea, and Iran possess the capabilities and interests to be of genuine concern. This means that enduring solutions cannot be Russia-specific.

Below are examples of specifically Russian-backed election interference, not offered to minimize other threats, but in order to illustrate the range of a single actor on a global scale and to situate the 2016 U.S. election interference in a broader context.

Ukraine 2014

In May 2014, four days before the scheduled national election, hackers associated with the Ukrainian-based Cyber Berkut group infiltrated computers at Ukraine's Central Election Commission and destroyed files essential to vote-counting.[3] Two days after the breach, the Ukrainian government said the system was repaired. On the morning of the poll, however, websites sending vote counts to the commission were hit with a denial-of-service attack later attributed to Cyber Berkut, delaying the vote count by several hours.[4] Following the election, government officials revealed that on the night the vote tally was announced, experts discovered malware in the commission's computers that would have incorrectly called the election for far-right leader Dmytro Yarosh with 37 percent of the vote and Petro Poroshenko with 29 percent. The government removed the malware before the commission released the official projections, which accurately showed Poroshenko to win with a majority of the vote, and Yarosh to win just one percent.[5] Notably, a Russian news outlet reported the results that the malware would have projected.[6]

Germany 2015

[3] "Authorities: Hackers foiled in bid to rig Ukraine presidential election results." *Kyiv Post*, May 25, 2014. https://www.kyivpost.com/article/content/may-25-presidential-election/authorities-hackers-foiled-in-bid-to-rig-ukraine-presidential-election-results-349288.html

[4] "Ukraine election narrowly avoided 'wanton destruction' from hackers." *Christian Science Monitor*, June 17, 2014. https://www.csmonitor.com/World/Passcode/2014/0617/Ukraine-election-narrowly-avoided-wanton-destruction-from-hackers

[5] *Id.*

[6] *Id.*

In 2015, the German parliament was hacked by the group known as APT28 or Sofacy[7]—the same Kremlin-linked group what would later target the U.S. Democratic National Committee and other groups during the 2016 U.S. election. The attack was designed to install malware to give intruders permanent access to the computers of members and staff and involved the theft of unknown amounts of data. The attack persisted for three weeks and included monitoring member and staff communications before it was detected. Because precisely what was stolen remains unclear, fears surfaced prior to the 2017 German elections that damaging information might be released in order to compromise or influence that process.[8]

Montenegro 2016

During the October 16, 2016, Montenegrin parliamentary elections, multiple media and government websites—including the website of Montenegro's top nongovernmental election observer[9] and sites affiliated with the governing Democratic Party of Socialists, which campaigned on further alignment with NATO—were targets of denial-of-service attacks. Despite allegations of Russian involvement, the Kremlin denied any connection.[10] In April 2017, the week that President Trump signed ratification papers officiating Montenegro's entrance into NATO, the U.S. government said there were "credible reports" that Russia tried to interfere with Montenegro's elections.[11]

France 2017

Two days before the second round of voting in France's 2017 presidential election, then-candidate Emmanuel Macron's *En Marche* party released a statement saying it was "the victim of a massive, coordinated act of hacking" as hackers released nine gigabytes of stolen emails from the left-leaning candidate's campaign.[12] Trend Micro, a

[7] "Russia 'was behind German parliament hack.'" *BBC News*, May 13, 2016. http://www.bbc.com/news/technology-36284447

[8] "Germany fears Russia stole information to disrupt election." *Politico*, May 6, 2017. https://www.politico.eu/article/hacked-information-bomb-under-germanys-election/

[9] "White House Readies to Fight Election Day Cyber Mayhem." *NBC News*, Nov. 3, 2016 https://www.nbcnews.com/news/us-news/white-house-readies-fight-election-day-cyber-mayhem-n677636

[10] *Id.*

[11] "U.S. says 'credible reports' Russia tried to interfere with Montenegro elections." *Reuters*, April 12, 2017. http://www.reuters.com/article/us-usa-trump-montenegro/u-s-says-credible-reports-russia-tried-to-interfere-with-montenegro-elections-idUSKBN17E22F

[12] "Macron Campaign Says It Was Target of 'Massive' Hacking Attack." *The New York Times*, May 5, 2017. https://www.nytimes.com/2017/05/05/world/europe/france-macron-hacking.html?_r=0

security firm, had said in April that a known group of hackers, which it called Pawn Storm, had targeted Macron's campaign in a phishing attack.[13] U.S. intelligence agencies and cybersecurity firms said that Pawn Storm was the group also known as Fancy Bear and APT 28,[14] an arm of Russian intelligence and one of two Russian government–linked entities that targeted the Democratic National Committee during the 2016 U.S. election.

These examples are non-exhaustive of the suspected Russian activity related to foreign elections over the past three years. They are intended to illustrate the breadth of activity of a single, committed nation state. They demonstrate that the election-security challenge is vast and that an effective policy response will require a range of technical, as well as domestic and international policy solutions.

Domestic Policy Considerations

To develop solutions, Congress must account for the domestic constitutional and political landscape. In the United States, state and local governments, rather than the federal government, primarily administer elections. The Elections Clause of the Constitution vests the states with regulatory power over elections, but allows Congress to "at any time by Law make or alter such Regulations. . . ."[15]

Notwithstanding the explicit override authority of Congress, perceived federal overreach is likely to meet strong resistance from states on political and policy grounds, if not necessarily constitutional objections. In 2016, at least one state declined even voluntary assistance from the Department of Homeland Security and went on to erroneously accuse DHS of improperly breaching state election systems.[16] In recognition of privacy sensitivities, another state's Secretary of State responded to requests from the Presidential Advisory Commission on Election Integrity for voter records by telling the commission to "go jump in the Gulf of Mexico."[17] Thus, voluntary efforts—those designed to be more carrot than stick—are more likely to be successful in the short-term.

[13] "Russia-linked hackers targeting French election, security firm says." *CBS News*, April 25, 2017. https://www.cbsnews.com/news/russia-hacked-french-election-trend-micro-report-fancy-bear-pawn-storm/

[14] *Id.*

[15] US Constitution, Art. I, Sect. 4, Clause I.

[16] "Correspondence Between DHS and U.S. Representative Jason Chaffetz." *Department of Homeland Security*. Dec. 8 2016-Feb. 28, 2017. https://www.dhs.gov/sites/default/files/publications/Correspondence%20between%20DHS%20and%20U.S.%20Representative%20Jason%20Chaffetz%20%28R-UT%29.pdf

[17] "Secretary Hosemann's Statement on Request for Voter Roll Information." *Secretary of State of Mississippi*. June 30, 2017. http://www.sos.ms.gov/About/Pages/Press-Release.aspx?pr=800

States are under-resourced in funding, training, expertise, equipment, and auditing capabilities. For example, according to the Brennan Center for Justice, forty-one states have voting machines that are more than ten years old. And while election officials in twenty-nine states express a desire to replace voting machines, 80 percent report a lack of secure funding.[18] There are also substantial variations not only between states, but also in some instances from county to county. Under these conditions, states cannot reasonably be expected to withstand sophisticated nation-state attacks—to not only counter known threats, but also to anticipate unknown threats. While respecting states' rights, the federal government must assume responsibility for providing necessary support.

The federal designation of election systems as critical infrastructure is a necessary but insufficient step. Former DHS Secretary Jeh Johnson designated election infrastructure as a critical infrastructure sub-sector of the existing government facilities sector on January 6, 2017.[19] This designation allows DHS to better prioritize services and support and to share intelligence information, but it does not supplement any regulatory authority.

Moving Toward Solutions

There are no obvious or easy solutions here. However, there are clearly areas where congressional action could lead to demonstrable gains. Below are recommended areas for congressional attention.

- *Develop a national strategy for securing elections.*

The United States should develop a national strategy to secure elections aimed at protecting systems, deterring bad actors, and bolstering public confidence.[20] This approach should empower state and local authorities and focus on defense-in-depth and resiliency by design. A successful strategy must not only work to prevent attacks, but also to implement systems to rapidly restore confidence in the event of an attack.

[18] "American Voting Machines at Risk." *The Brennan Center for Justice.* June 12, 2017. http://sites.nationalacademies.org/cs/groups/pgasite/documents/webpage/pga_180930.pdf

[19] Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector, Jan. 6, 2017. https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical

[20] For additional analysis, see David P. Fidler, Presentation for the National Academy of Sciences Committee on the Future of Voting, available at https://livestream.com/accounts/7036396/events/7752647.

This strategy must balance security with other important objectives, such as preserving and promoting voter access.

A strategy that sets neutral standards and thresholds well in advance of the next national election can help avoid politicization. The 2016 election demonstrated how the fear of even a perception of political motivation can inhibit the executive branch from responding to known threats. Setting standards for baseline security, recount and auditing thresholds, and deterrent response options will strengthen public confidence and avoid excessive inhibition where nation-state attribution or response is necessary.

- *Provide federal resources in the form of funding, support, and best practices.*

Additional federal resources designed to improve election security should be made available to states on a voluntary basis. Currently, the Senate has offered amendments to the National Defense Authorization Act that would take this approach.[21] These resources should be contingent on implementing security measures aimed at long-term sustainability. Additional federal support should be conditioned on meeting federally developed best practices for election administration and security. Best practices would include the use of paper ballots, routine audits, training, and penetration testing.

- *Regulate election-technology vendors.*

Both federal and state governments must better regulate the commercial industry surrounding elections. Currently, this is a limited and proprietary market that too often leaves states with insufficient power to dictate security standards. In addition to setting standards for secure design, manufacturing, and storage of voting systems, the government must mandate ongoing processes such as routine penetration testing. Election technology vendors should also be required to promptly report any discovered vulnerabilities to state election officials and the Department of Homeland Security. At the same time, Congress must eliminate the legal barriers to independent vulnerability research contained in the 1998 Digital Millennium Copyright Act and the Computer Fraud and Abuse Act.

- *Lead the development of international norms against election interference.*

The United States should lead to establish international norms against election interference. Such norms can differentiate between espionage—which is an accepted

[21] Protecting Electoral Infrastructure–Klobuchar/Graham and the NDAA, *Lawfare*, Sept. 5, 2017. https://www.lawfareblog.com/protecting-electoral-infrastructure%E2%80%93klobuchargraham-and-ndaa

international practice—and active measures or covert influence operations. There are instructive prior examples, such as agreements on norms against commercial espionage. But heeding this suggestion means that the United States must embrace a policy of self-restraint in order to develop the necessary international consensus. Some have pointed to past allegations of U.S. activity in foreign elections. Rather than focus on the distinct factual situations in which such activity might have occurred, effective policy should clearly articulate which activities the United States and international community deem unacceptable and include assurances that the U.S. will not itself engage in such behavior.

- *Renew and sustain political commitment to the issue of election security.*

Finally, Congress, as our primary elective body, must recalibrate the political climate surrounding election security if progress is to be made. It must reestablish norms that have been broken, and demand that candidates behave more responsibly in discussing elections moving forward. If we persist in describing elections as "rigged," in tolerating the suggestion that a candidate is not bound to accept an election outcome if he or she does not win, and in demeaning the conclusions of the U.S. and allied intelligence communities, then we ourselves will create the conditions for a crisis of public confidence. Opponents of liberal democracies will not hesitate to exploit that opportunity.

Thank you again for the opportunity to address these subcommittees. I look forward to taking members' questions on this important national security issue.

Mr. HURD. Thank you.

And to start off our first round of questions will be the distinguished gentleman from Alabama, Chairman Palmer. You're recognized for 5 minutes.

Mr. PALMER. Thank you, Mr. Chairman.

Dr. Blaze, what do you think is the biggest takeaway from the DEFCON report?

Mr. BLAZE. So I think the biggest takeaway is both alarming and yet unsurprising, and that is that vulnerabilities that we knew in principle were present are, in fact, exploitable in practice by nonspecialists.

Mr. PALMER. Here's a question that I'm going to direct to you but some others may want to respond to it. I'm very concerned about foreign influence on our elections. But we—to the last year, particularly the last few years, we've had hundreds, if not thousands, of reports of domestic voter fraud, whether it's voter register, it's manipulation of ballots at the polling place. Is that not also a threat to our elections?

Mr. BLAZE. Well, certainly, you know, the potential threats to our election are very broad, and they include everything from the voter registration process through the reporting of election results. My concern as a computer scientist, and my expertise, is particularly on the technical vulnerabilities present in these systems as they're designed and built. And what, really, every expert who has looked at these systems has found is that the attack surface of these machines leaves us particularly vulnerable——

Mr. PALMER. But not just to foreign——

Mr. BLAZE. —adversary——

Mr. PALMER. But not just to foreign interference but domestic interference as well. Wouldn't you agree?

Mr. BLAZE. Absolutely. A determined domestic adversary——

Mr. PALMER. So someone with a political agenda could—if they had the technical expertise, would be as much a threat as a foreign entity. Would that be a reasonable conclusion?

Mr. BLAZE. That's right. Particularly someone interested in disrupting an election, or casting doubt on the legitimacy. The way these systems are—particularly DRE-based systems are designed, it's very difficult to disprove that tampering has occurred. And, ultimately, that's a critical aspect of being able to have confidence in the result.

Mr. PALMER. One of the things that particularly concerns me is, is that you can be disconnected from the internet, from WiFi, and still hack a machine because of the potential of parts within the machine, foreign-manufactured parts. Can you talk briefly about that?

Mr. BLAZE. That's right. The design of DRE systems makes their security dependent not just on the software in the systems, but the hardware's ability to run that software correctly and to protect against malicious software being loaded. So an unfortunate property of the design of DRE systems is that we have basically given them the hardest possible security task. Any flaw in a DRE machine's software or hardware can become an avenue of attack that potentially can be exploited. And this is a very difficult thing to protect.

Mr. PALMER. Do we need to go to, even if we have some electronic components, to back it up with paper ballots? Because your fallback position is always to open the machine and count the ballots.

Mr. BLAZE. That's right. So print and counted optical scan systems also depend on software, but they have the particular safeguard that there is a paper artifact of the voter's true vote that can be used to determine the true election results. Paperless DRE systems don't have that property, so we're completely at the mercy of the software and hardware.

Mr. PALMER. As inconvenient as it might seem, I mean, for years and years and years, we relied on paper ballots. It doesn't seem unreasonable that that would be a great safeguard.

I want to ask Secretary Schedler and Cortes about this. In Alabama, it's a mixture of voting machines. Do you have that as well? I mean, do you have kind of an all over the roadmap?

Mr. SCHEDLER. Congressman Palmer, Louisiana is what we call a top-down system. We control, as I indicated in my opening comments, all of our own machines. We warehouse our own machines. You know, we do have a tape system of paper behind that that we can audit specifically with three different types of processes. It has never been unproven in a court of law. And the only thing I want to add to the DEFCON is that, look, I welcome anyone from the academic side to look at any system. But let's put it in contents. The contents is an unfettered access to a machine that's given to them in a laboratory. Let's talk about when you discover—and I'm certain the professor from University of Pennsylvania, or MIT, or anyone, if I gave them unfettered access to a machine can figure out how to tinker with that machine or disrupt it. That machine.

In Louisiana, as most States, the machines are not linked together. Each one has a separate cartridge to itself. And I guess the implication is that at the point of programming, you could do something to that. I guess that's possible, and I wouldn't argue that point with someone much more learned on that subject than I.

But, again, in a top-down system, that would mean someone in my office, on a computer that is cleaned and scrubbed before an election and after, would have to have access to that program and equipment in my office.

The other thing that's never mentioned in any of the hacking of a machine is after you figure out what you're going to do, has anyone yet ever sat down and discussed—and I'll only give you Louisiana—in roughly a 36-hour period, after we go into the machine, put a metal clamp like you have an on your electrical box at your home, with a serial number, figure out they're going to get into 64 warehouses across my State, go into 10,200 machines, undetected under camera, no one saw you, unscrew the back of the panel, do what you're going to do, put the panel back on, and figure out how you're going to put that metal clamp back on.

So the point I'm making is that a lot of these things that we talk about are certainly possible. But I would suggest to you the amount of people you'd have to put in play to commit this fraud, it would be easier to do a stump speech and basically convince them to vote your way, the legal way.

Now, there is no such thing as a perfect election. None. There are issues that occur from electricity going out, to fires at a precinct—I could go on and on—flooding in Louisiana and the like. But, you know, one of the things that everybody has to understand is all of these conversations around this all deter voter participation, whether you believe it or not.

Mr. PALMER. Let me just say this, Mr. Chairman. I appreciate your answer, Mr. Secretary. Is that a couple of things that I hope that we're sensitive to. One is that we don't want the Federal Government's involvement in this to infringe upon the State's authority to conduct elections. And then the other is, is that we don't want to just be so focused on foreign interference that we don't give due diligence to addressing the domestic threat as well.

I yield back.

Mr. HURD. Ranking Member Kelly, you're now recognized.

Ms. KELLY. Thank you, Mr. Chair.

Mr. Krebs, I wanted to ask about your agency's efforts, DHS, to notify 21 States about Russian attacks on their State election systems. On October 20, Ranking Member Cummings and I sent a letter to DHS requesting copies of the notifications you sent to 21 States that were attacked before the last elections.

And, Mr. Chairman, I ask for unanimous consent that this letter be made part of the official record for today's hearing.

Mr. HURD. So ordered.

Ms. KELLY. In our letter, we also asked for other materials, including all documents, and I quote, "relating to Russian Government-backed attempts to hack State election systems." Our letter asked for these documents by October 31, but we got nothing. So earlier this week, the Republican committee staff kindly agreed to help us make crystal clear to DHS that we wanted these documents before today's hearings so we could ask informed questions. DHS assured us that they would respond. Instead, late in the day yesterday DHS sent us only an email with a short script that DHS employees apparently read over the phone to State election officials.

Mr. Krebs, I'm just asking, where are the rest of the documents that we requested?

Mr. KREBS. Ma'am, I'm aware of the script that was provided. A lot of those notifications were over the phone. They were not via email. There may have been some follow-up conversations. As to the rest of the documents, if you'll permit me to go back, and I commit to you that we will have a more fulsome answer for you. But as to the specifics of each document, I would have to go back and check on that.

Ms. KELLY. Okay. I'm counting on you——

Mr. KREBS. Yes, ma'am.

Ms. KELLY. —to deliver. Because the telephone script is literally only 13 sentences long. It does not refer to any specific State or any specific attack. It is just a generic script that provides no additional information at all.

And, you know, just curious about where are all the supporting documents that we requested that set forth the details of the attack? And, with all due respect, the telephone script does not help us do our job, which will help you in turn.

You have not provided us with any information about the tools the attackers used, or the tactics that they utilized, or any information on the results of your conversations with these States or the steps you took to follow up. So it's been more than a month since we asked for those documents, and the majority wants those documents also. Can you tell us what the holdup is?

Mr. KREBS. Ma'am, I'm not aware of any particular holdup. What I will say is the nature of the conversations we've had over the last, frankly, year with the States—and I've had a number of conversations with Secretary Schedler, my team has regular conversations with Commissioner Cortes, and a range of other State election officials. When you characterize these things as attacks, I think that that is perhaps overstating what may have happened in the 21 States as was mentioned over the course of the summer.

The majority of the activity was simple scanning. Scanning happens all the time. It's happening right now to a number of probably your websites. Scanning is a regular activity across the web. I would not characterize that as an attack. It's a preparatory step.

In terms of those scripts, there are two scripts. One script was provided to States that wanted additional information if they were included in that batch of 21. And in the other script is for those States that were not in that batch of 21. So if that context was not provided, I apologize, and I'm happy to follow up and make sure that you get the information that you're looking for.

Ms. KELLY. Okay. And I just want to make sure the chairman is willing to work with me today by directing DHS to provide all the documents actually within 1 week, and that I hope we can work together to get these documents as soon as possible, hopefully in 1 week. Because this hearing is supposed to be about cybersecurity of voting machines and our investigation should be bipartisan. Yet, DHS is withholding the very documents that would help us, on both sides of the aisle, help our committee understand how our State election systems were attacked by the Russians. So I look forward to your cooperation and working with my chairman.

I yield back.

Mr. HURD. Would you yield to me?

Ms. KELLY. Of course.

Mr. HURD. Mr. Krebs, was there anything other than scanning done at those 21 locations?

Mr. KREBS. The vast majority of those 21 States were, in fact, scanning. There was a very small subset of those groups that there was a compromise on the voter registration side, but not within the tallying. And then there was some additional—a small group, also, that had some targeting. So we actually winnowed it down.

Now, when we talk about that scanning, it was not, also, necessarily an election system that was scanned. That's additional context that we provided to our partners in the State election offices. What we saw in a lot of those cases was, frankly, drive-bys. It was—you know, you think about walking down the street, and you're looking for a house. You knock on the door. You don't know what's there. You may be looking to get into the neighbor's house, looking for a key. I apologize for the kind of mundane analogy. But that's simply what we saw was doing a drive-by, seeing what was there, seeing if the door was locked. In a lot of the cases, as Secretary Schedler pointed out, there was adequate protections involved.

Mr. RUSSELL. So, Mr. Krebs, you'll be able to provide us with the details of who was in addition to scanning and what the nature of that contact was?

Mr. KREBS. In terms of the States that were targeted or scanned, that's a difficult conversation because the information is provided to us based on trust, just like all our other relationships with the critical infrastructure community. The fact that we don't have statutory authorities to compel, we are engaging on a trust-based relationship here. If I then turn around and share information that Tom provided to me outside of the scope of that confidential relationship, Tom will never share with me again.

In fact, Edgardo will never share with me again. And this is going to jump out of this relationship. And the entire cybersecurity mission of the Department of Homeland Security, it is a voluntary mission. That entire mission will be jeopardized if we divulge confidential information.

So I am happy to provide contextualized information on the nature of those 21 States. But in terms of the 21 States, I suggest you reach back to your—and I will help with you to reach back to your States—ma'am, you mentioned that your State may have been one. I will help you have that and facilitate that conversation. But today, while we're sitting here, I also encourage you to ask my counterparts here from the States.

Mr. HURD. Mr. Duncan, you're now recognized for 5 minutes.

Mr. DUNCAN. Thank you very much, Mr. Chairman.

I want to go back into this DEFCON conference from this past July. The article that I have said participants tested over 25 pieces of election equipment, and every piece was effectively breached in some manner. And it says in the DEFCON report on the voting machine hacking, the results were, quote, "By the end of the conference, every piece of equipment in the voting village was effectively breached in some manner. Participants with little prior knowledge and only limited tools and resources were quite capable of undermining the confidentiality, integrity, and availability of these systems.

And back just a few months ago when they had the worldwide cyber attacks, I don't often quote a liberal—don't often quote liberal magazines in here, but Robert Kuttner, the editor of The American Prospect Magazine, he wrote this. This was written in The Huffington Post. He said, "Last week's cyber attack to produce the wrong reasons"—"the wrong lessons." The immediate takeaway seems to be that large institutions need much better cybersecurity systems. But there's a much simpler and better solution. Vital systems that can't withstand the catastrophic risk of malicious hacking should just go offline. Hackers will always be able to find ways of getting into network systems. The fantasy of ever-better cybersecurity is delusional. We could spend half the GDP on network security and someone will still find a way to breach it.

I know that we have addicted almost everyone in this country to the computers and the iPads and so forth. But I tell ya, I believe that cybersecurity is a multi-billion-dollar hoax. And I'm sure what we're going to do, we're going to spend untold billions trying to come up with these systems that, as Mr. Kuttner says, it's a fantasy.

And I think the solution should be that we should go to the Canadian system. I read several years ago that they had much smaller precincts. They're usually on average of 500 people per precinct, and they use paper ballots. And I know that's old fashioned. But I think we're headed down the wrong path here. It's a path that I'm sure we're going to go on. But I think that—I agree with Mr. Kuttner and also the findings of this DEFCON report.

Anybody want to say anything?

Mr. SCHEDLER. I'll just say Louisiana is not one of the 28 States—21 States. Excuse me. So you can scratch one off.

Mr. HURD. Thank you.

Mr. DUNCAN. All right. Well, I yield back, Mr. Chairman.

Mr. HURD. Ranking Member Demings, you are now recognized for 5 minutes.

Mrs. DEMINGS. Thank you so much, Mr. Chairman.

You know, as we continue this discussion today, I cannot help but think about my own parents. My mother was a maid, and my father was a janitor. They didn't have a lot that other people had, but they did have their votes. And I cannot remember an election growing up where they did not cast that vote. They believed that it mattered. And I would hope that every witness here today and every member of our subcommittee, regardless of if you were a billionaire or a maid and a janitor, that we would all work to protect the integrity of our voting system in the greatest country in the world.

So, Dr. Blaze, I want to go back to the DEFCON report that we've talked quite a bit about today. And I certainly listened to some of the comments my colleague, Mr. Duncan, made about how these systems were breached. But could you please talk a little bit more about the equipment that was used to breach the systems? Was it sophisticated equipment or not? And what kind of prior knowledge did the breachers have, if any at all?

Mr. BLAZE. So, first of all, I'd like to point out the DEFCON Voting Village was not intended to be a formal security assessment. It was an informal opportunity for people from a broader community, really for the first time, to get access to actual voting equipment.

We got about five different models of voting machine and electronic poll book, made them available. We made available the reports that had been published about these equipments in some cases. And that was it. We opened the doors on Friday afternoon, and people came in and any tools and equipment that they brought to that, they were—they had to bring in themselves. There was no access to any proprietary information, no computer source code was available. Just the equipment and electricity.

Mrs. DEMINGS. And I know some or many have criticized or questioned the vulnerability of the ability to hack the systems because of the decentralized nature of the machines. Do you agree that the decentralized nature of our elections protects us from disruption or not so much?

Mr. BLAZE. You know, it's a double-edged sword. The fact that we have highly heterogeneous systems that are decentralized in their administration makes it difficult for somebody to do a single thing that will affect us on a national scale. And that is, in fact, an important safeguard. But it cuts both ways. There's, in fact, only a relatively limited number of different models of voting equipment used in the United States. And an adversary, particularly a foreign state actor interested in disrupting our election process, has the luxury of being able to pick the weakest systems and need only find the most poorly administered and the most vulnerable systems to do sufficient damage to suit their needs. So while it may make us more secure against somebody with one-stop shopping disrupting a national election, it actually increases our vulnerability to some disruption happening, perhaps sufficient disruption that we don't have confidence in the outcome.

Mrs. DEMINGS. We've heard a lot about the need for an audit. What type of audit do you believe would have to be performed on a paperless voting machine to verify the vote counts or verify that the vote counts had not been altered?

Mr. BLAZE. So paperless voting machines essentially are voting computers that are completely dependent on the software that was running on them at the time of the election. There is no fully reliable way to audit these kinds of systems. We may get lucky and detect some forensic evidence. But, ultimately, the design of these systems precludes our ability to do a conclusive audit of the voter's true intent. That's why paperless systems really need to be phased out in favor of things like optical scan paper ballots that are counted at the precinct but backed by an artifact of the voter's true intent.

Mrs. DEMINGS. Thank you, Dr. Blaze.

And, with that, I yield back.

Mr. HURD. Mr. Mitchell, you're recognized for 5 minutes.

Mr. MITCHELL. Thank you, Mr. Chair.

Mr. Krebs, could you help me with one thing? On June 21st, Secretary Johnson—and this is a quote—appeared before the House Permanent Select Committee on Intelligence. He said: "To my current knowledge, the Russian Government did not, through any cyber intrusion, alter any ballots, ballot counts, or reporting of election results." Has anything changed since that point in time that you're aware of?

Mr. KREBS. Not to my knowledge. No, sir.

Mr. MITCHELL. So you have received no information that the election results, either at the Federal level or the States you looked at, were altered in terms of counts or outcomes?

Mr. KREBS. No, sir, I don't have any additional or contrary information to——

Mr. MITCHELL. Do you have any indication that any actor, be they foreign agency or domestic, actually attempted to influence the vote counts or ballot activity?

Mr. KREBS. Sir, I believe that's a different question.

Mr. MITCHELL. Yes. You're correct.

Mr. KREBS. My understanding, the intelligence assessment is that a foreign adversary—now, if I can back up. You said June. June of 2016?

Mr. MITCHELL. 2017. June 21, 2017.

Mr. KREBS. So former Secretary Johnson.

Mr. MITCHELL. Former Secretary. I'm sorry, yes.

Mr. KREBS. So since then, any opportunity to influence, is that your question?

Mr. MITCHELL. The question is, did you find any indication that there was any effort to, by domestic or foreign influence, to affect the ballot results since that point in time?

Mr. KREBS. No, sir.

Mr. MITCHELL. Thank you.

Let me ask the group as a whole. I think the consensus is that the integrity of our election is a national infrastructure issue. Anybody disagree about that? It's every bit as important as our roads, our ports, our waterways. You know, we don't invest any Federal money, never mind Federal standards or some guidelines on that. Is anybody opposed to the idea that we go forward with some form of a—we invest to support that program with some kind of guidelines the States can choose to whether they want to participate or not?

Mr. SCHEDLER. I think best practices would be a better word to use. I think that the States as a whole—and I speak in a nonpartisan fashion——

Mr. MITCHELL. Sure.

Mr. SCHEDLER. —would be adamantly against an intrusion of the Federal Government——

Mr. MITCHELL. Oh, I agree.

Mr. SCHEDLER. —of course we would do it, because it's in the Constitution. But certainly best practices. I think there are a lot of evidence of that with some of the entities that are out there today. We welcome additional ones. Certainly, we're not——

Mr. MITCHELL. Let me clarify for you, Secretary. I wasn't suggesting that we impose a system on the States, simply we have a grant program with a range of options, and States, particularly areas——

Mr. SCHEDLER. Usually, the grant programs have strings attached.

Mr. MITCHELL. Well, if the grant program said, do you want to update your equipment, and it meets certain sets of expectations and security, you can choose to do it or not.

Mr. SCHEDLER. Right.

Mr. MITCHELL. If you don't——

Mr. SCHEDLER. If it's voluntary and we can accept it, and we can accept whatever strings come with it, and you can turn it down, I have no problem.

Mr. MITCHELL. Commissioner Cortes, you have any feedback on that?

Mr. CORTES. Yes, sir. I think resources for States to either purchase equipment, or for those that have already moved to equipment to do other things to strengthen the security of the election, whether it be electronic poll books or a registration system, would be greatly appreciated and something that we would certainly support.

Mr. MITCHELL. It just occurs to me, why don't we do that for our highways. We do that for our ports. But yet we expect magically the elections are going to happen with local resources, without, frankly, minimal support.

Let me give you an example. Mr. Duncan talked about would we not be better off with paper ballots. You have any feedback on simply going to a full paper system or some system that's paper dependent?

Mr. SCHEDLER. And you're referring to a paper system at a poll location, not a mail paper ballot?

Mr. MITCHELL. Correct.

Mr. SCHEDLER. Okay. I'm not opposed to that. Matter of fact, the system that we're looking at—we're not out for bid yet—would be one that would produce—even though you would vote on an electronic machine, it would produce an actual paper ballot——

Mr. MITCHELL. My whole concern with that——

Mr. SCHEDLER. —and then a cast ballot only with that point when you put it into a secure box.

Mr. MITCHELL. My concern with that, and Dr. Blaze makes the point, is that if you produce a paper result after you put something into the machine, if, in fact, the machine is tampered with, you could, in fact, end up just confirming the tampered information.

Mr. SCHEDLER. Yes, sir. But we do have, currently, at least in the machines I use, a paper—I don't want to call it a cash register receipt, but for just the purposes of this meeting—that we can produce and audit back. So there's several audits even though I don't have a paper ballot of Mr. Mitchell, I can certainly use that in a court of law, and we have been very effective with that.

Mr. MITCHELL. Well, as Dr. Blaze states——

Mr. SCHEDLER. There's one thing I want to do mention. In this whole conversation is the segregation of the vulnerability side of the registration, or a poll book versus voting day. No State—no State—votes online in cyberspace.

Mr. MITCHELL. I know that.

Mr. SCHEDLER. So how do you attack something in cyberspace that's not in cyberspace?

Mr. MITCHELL. Right.

Mr. SCHEDLER. And there's one or two exceptions to that, Alabama with military voting, Alaska, in some remote areas. And I think there's one other State. But a minuscule amount of votes.

Mr. MITCHELL. Let me—time—deference, Mr. Hurd?

Mr. HURD. [Nonverbal response.]

Mr. MITCHELL. I understand, and I think Dr. Blaze's suggestion that an optical scan system allows you to have the original source document that says, you know, voter number 028 voted this way. So that, in fact, you don't depend on the system to generate it. But that's something we can deal with.

Question, you all are aware of what happened in Michigan in terms of the Federal election, that 60 percent of the precincts in the city of Detroit, they couldn't do a recount because the numbers didn't match?

Mr. SCHEDLER. No, sir, I'm not aware of that.

Mr. MITCHELL. There were more voters that voted—admittedly, only 728, nevertheless. There were more votes counted than there were voters, and there were 328 that were listed as voting but the ballots never showed in the count. That meant that 60 percent of the precincts in the city of Detroit weren't auditable.

I guess my point is, is you couldn't do a recount. I think something we need to encourage the States to do is have an audit system where we raise these issues of why those disparities, and how we prevent them. Because that's—if, in fact, we need to do a recount, it was not possible to do within the city and several other jurisdictions.

I'll submit for the record, Mr. Chair, the article—I'll have this submitted for the record—of what transpired in Detroit, which was a paper-then-scan system. They still managed to lose enough votes that they couldn't recount.

Mr. KREBS. Yes, sir. And I brought that out in my comments. Even with a paper system, you still got to have some good protocols. It's not foolproof by any means.

Mr. MITCHELL. Agreed. Agreed.

Thank you, Mr. Chair, for the deference, and I yield back.

Mr. HURD. The distinguished gentleman from the State of Missouri, Mr. Clay, you are now recognized for 5 minutes.

Mr. CLAY. Thank you, Mr. Chairman. And I want to thank the witnesses for your testimony today.

Last June, the vice chair of the Presidential Advisory Commission on Election Integrity, Chris Kovach, made an extraordinary request of all State election directors to transmit to the White House the confidential information and voting history of all Americans living in their State. Mr. Kovach directed the State elections officials to provide the sensitive data to a government email address with no apparent means of securing that data.

Dr. Blaze, please explain the data security issues with transmitting sensitive voter data over email.

Mr. BLAZE. Well, I'm not familiar with the precise nature of the request. But as you've described it, certainly sending that kind of information over an ordinary unencrypted email system would be fraught with many security and privacy issues.

Mr. CLAY. If confidential voter data were revealed due to insecure transmission, could that provide means to infiltrate State election systems?

Mr. BLAZE. Yes. That sort of information would—could potentially be quite valuable to an adversary interested in targeting particular polling places or individuals or areas. So information about historical voting patterns and about individual registered voters can be quite sensitive.

Mr. CLAY. I see.

Secretary Schedler and Mr. Cortes, I understand your States did not comply with Mr. Kovach's request. Could you explain why?

Mr. CORTES. Congressman, that's correct. Virginia did not provide any data that was requested from the Commission. We had significant concerns related to the sweeping nature of the request. And, you know, we spent a lot of effort and lot of resources protecting our voter data of Virginians. So to take that and turn it over to a Commission with no sense of what it was going to be utilized for, how it was going to be stored and maintained, raised significant concerns for us. And so we declined to provide anything whatsoever.

Mr. CLAY. Thank you for that.

Mr. Schedler?

Mr. SCHEDLER. Mr. Congressman, we likewise refused that. But I do want to clarify one thing that has been lost in this whole debate. And why Mr. Kovach, my colleague, did not early-on clarify his position. I watched him for 4 days on national news networks. But if you go back and look at the original request, he truly didn't ask for that. What he asked for was what was available publicly under State law. And then, after that, instead of putting a period, he went on with Social Security number and other—why he did that, I don't know. He caused me a lot of heartburn in my State with thousands of emails and Facebook posts and the like.

So to answer your question, no, I did not supply that to him. I told him for $5,000 and a credit card, we'd be glad to supply him the public informational data that you could get on anyone from Google, quite frankly more information. But you're correct, putting that out in the fashion it was.

But I do want to say this: It wasn't just the Trump administration that asked for that. I was posed with that under three defiances to a Federal judge to produce that under President Obama's administration through a Department of Justice——

Mr. CLAY. I see.

Mr. SCHEDLER. —in a lawsuit from several entities. And I refused President Obama, and I refused President Trump. So I am consistent.

Mr. CLAY. Well, let me ask you. That brings me to another question for you and Mr. Cortes.

Are you aware of any cases of voter impersonation in your State? Mr. Cortes, you can take it first.

Mr. CORTES. Congressman, I'm not aware of any instances of voter impersonation taking place in Virginia. No.

Mr. CLAY. So no pending cases or anything like that?

Mr. CORTES. Not that we're aware of, sir, no.

Mr. SCHEDLER. No, sir. We wouldn't in Louisiana. I mean, we have some issues. But let's put it this way: If we have had one, it's never been prosecuted or been able to be proven.

Mr. CLAY. Don't you think it's a little difficult to get enough voters to show up, let alone someone showing up and impersonating someone else?

Mr. SCHEDLER. Well, I think the real issue is—and, alluded again, we separate the distinctions in the election system. The registration side, list maintenance, some States do a better job than others. I know our current President has alluded to 3 to 5 million voters. What he's referring to is 3 to 5 million potential voters on registration lists. The voter fraud would be one of those individuals who shouldn't be on there showing up at the poll and voting. It may be that. It may be more. It may be less. But——

Mr. CLAY. But you and I know people have the same names.

Mr. SCHEDLER. Yes, sir. Yes, sir.

Mr. CLAY. So that shouldn't disqualify them from being——

Mr. SCHEDLER. No, but that's why we have identifying information——

Mr. CLAY. —a qualified registered voter.

Mr. SCHEDLER. —like mother's maiden name, Social Security number, date of birth, that we can distinguish those differences.

Mr. CLAY. Sure. All right.

Mr. SCHEDLER. Like in the State of Louisiana, we have a bunch of Heberts and Thibodeauxs, but we can distinguish it by a birthday or mother's maiden name.

Mr. CLAY. Well, look, I thank you all for your engagement, and my time is up. Mr. Chairman, I yield back.

Mr. PALMER. [Presiding.] I thank the gentleman.

Just a point of clarification. You did have reports of illegal voting in both your States. In Virginia, you had over 1800 illegals that apparently were reported voting. Is that correct, Commissioner Cortes?

Mr. CLAY. Mr. Chairman, I asked about voter impersonations, someone else showing up and saying that they are someone other than who they are.

Mr. PALMER. Thank you.

Mr. CLAY. And you know that's what the photo ID laws are all about.

Mr. PALMER. Right.

Mr. CORTES. Congressman, I believe you asked about our reports regarding illegal voter. We don't agree with neither the findings of the report, or, frankly, how the analysis was done. There are a lot of problems in there that we have indicated publicly. You know, in terms of proving, or, you know, identifying individuals that are citizens or not on the voter rolls is exceptionally difficult. And the processes that we have in place in Virginia, I think, capture and prevent anybody from voting illegally or improperly. And so the report you're referring to, I think, was very faulty in its analysis and really took information and made sweeping general statements without taking into account the reality, despite our best efforts to communicate with the report authors about it.

Mr. PALMER. Thank you.

In Louisiana, it's either Hebert or Hebert. So I can understand the problem you have there.

Mr. SCHEDLER. Depending on what part of Louisiana.

Mr. PALMER. The chair recognizes the gentleman, Mr. DeSaulnier, from California, for 5 minutes.

Mr. DESAULNIER. Being from California, I wouldn't recognize either version.

I just want to thank the chair, and I want to thank all of the people who are testifying in front of us today. And for the Secretary, I both agree with you, but maybe we have a small difference of opinion. The importance of the integrity of the voting process is obviously supreme for all of us sitting in this room. But raising legitimate concerns about the integrity of that, making sure that we are pursuing best practices in a world that's changing dramatically, I think, is what we're all concerned with. So in that regard, I'm hearing two sort of versions of things here from the panel.

And, Ms. Hennessey, in your research—I got a quote from Michael Vickers, who used to be the Pentagon's top intelligence official, who said, quote, "This attack is really the political equivalent of 9/11. It is deadly, deadly serious." The attacks that we have seen both against the United States, in my view, but also against western democracy. And this goes to undermining democracy. So we want to make sure, I would think, in Congress, that we're doing everything to make sure that we're ahead of it and questioning our existing system.

So you made a number of suggestions. First off, is there any doubt in your research that these hacks are attributable to Russia, these significant hacks?

Ms. HENNESSEY. Certainly, the intelligence community—the intelligence community assessment of the 2016 election assesses that with high confidence that is supported by a large body of public data. And there is no public information that would counter or refute that conclusion.

Mr. DESAULNIER. So keeping in mind that we're talking about, in this hearing, the title is Cybersecurity of Voting Machines, and we've got lots of other activity going out there that hopefully we'll discuss further in Congress, vis—vis the things we're learning about social media and data collection. But for this purpose, are we ahead of the game in your research? I read where the French and other western democracies are being much more aggressive, not knowing what their infrastructure is. But from your research, is the United States doing everything we can compared to other international democracies who are aware of the problem?

Ms. HENNESSEY. I think the short answer is no. There are two categories in which we can think about the U.S. response. What we've been talking today can broadly be categorized as deterrence by denial. So imposing security standards that make it difficult or impossible for the adversary to achieve their goals. Dr. Blaze and the others, I think, have pretty well articulated the insufficiency of the U.S. response on that front, the need for more to be done in terms of Federal resourcing, and at the State level.

There's also a broader concept of deterrence, right? So deterrence through setting international norms, response options. We are also not seeing sufficient buy-in, frankly, from the top at this point to push those efforts forward in order to get the international community both to agree on the seriousness of what occurred, and also to impose measures, including those passed by Congress, to ensure that it doesn't happen again.

Mr. DESAULNIER. I appreciate that.

Mr. Krebs, in that sort of vein, your response to Ms. Kelly is seen somewhere in-between. We know the uniqueness of the relationship as you have described it between State's rights and the ability for them not to feel like we're imposing on them. However, you've also talked about best practices. And it would strike me that you're in a position to be able to acquire those best practices, particularly in conversation with the intelligence community.

Ms. Kelly asked you if you would give us those documents. It seems like you're equivocating. Something—basically, you said in order to have a relationship with the States, it's based on trust. But forgive me for inferring from that there's a lack of trust in giving those documents to Congress. In a Federal election, it strikes me that Congress and the Federal Government has a requirement to make sure that we are pursuing best practices in partnership with the States, not overruling them. But if Congress asks for documents, including the minority party, it strikes me that you should give that to us, to the whole committee, without edits, without comments.

Mr. KREBS. Sir, if I may, I'd like to clarify to the ranking member, the information—ma'am, I'm glad you're here.

The information that I would provide, no question best practices. I've got them right here. Best practices are just fine to share. What we're talking about is the trusted information that's shared on the nature of what may have been a scan or a compromise. That's the information.

We have no question of the oversight interest of the committee, absolutely no question. The balance we have is the operational admission of the Department in partnership with our State and local partners in that—again, that overarching cybersecurity mission of the Department in working with our partners in a voluntary basis.

Mr. DESAULNIER. I'll take that as we'll receive the documents soon. So thank you.

Mr. KREBS. Yes, sir.

Mr. DESAULNIER. Thank you, Mr. Chairman.

Mr. HURD. [Presiding.] Mr. Krishnamoorthi, you are now recognized for 5 minutes.

Mr. KRISHNAMOORTHI. Thank you, Chairman Hurd and Palmer, along with Ranking Members Kelly and Demings, for convening today's important hearing. The sanctity and security of our election systems are the bedrock of our republic. The American people need to know, not just believe, but they need to know for certain that their votes are counted fairly.

My home State of Illinois was one of 21 States that the Department of Homeland Security informed us was targeted by hackers in June of 2016. The NSA reported that personal files for over 90,000 Illinois voters were illegally downloaded by Russian hackers. Mr. Krebs, do you have any reason to dispute the NSA's findings that Russian-affiliated entities were behind the recent election data breaches?

Mr. KREBS. I'm, unfortunately, not able to comment on that specific disclosure. That, I would, unfortunately, have to defer to the NSA.

Mr. KRISHNAMOORTHI. But do you have any reason to believe they're incorrect about that?

Mr. KREBS. I'm not certain to the nature of the report you're discussing. I, unfortunately, would have to, again, defer to the NSA to comment specifically——

Mr. KRISHNAMOORTHI. Right. You'd defer to the NSA because they are expert in this particular matter, and they have the intelligence and the ability to ascertain whether these data breaches occurred and who were the source of these data breaches, correct?

Mr. KREBS. Again, I would defer to the NSA on any discussion here.

Mr. KRISHNAMOORTHI. Sure. While the implications—and you're correct to defer to them.

While the implication of Russia's attack on one of our elections systems are concerning, what I find even more disturbing is that it was part of a broader international campaign to undermine western democracies such as the 2017 elections in France and Germany, as well as recent elections in the U.K. and other NATO countries.

Now, Mr. Krebs, again, I'd like to ask you a follow-up question. Can you assure me that DHS is working with our allies and the broader international community, the intelligence community, to develop a coordinated response to these incursions?

Mr. KREBS. So what I can speak to is the nature of the Department of Homeland Security's engagements with our international partners. Immediately before the French election, we reached out to the CERT, the French CERT, which is the Computer Emergency Response Team, keeping in mind that my responsibilities in this space are, frankly, two things: information sharing and technical support on a voluntary basis. So information sharing with the State and locals and also information sharing with the French CERT.

In terms of a broader strategy for pushing back, I'd have to defer to the interagency or the White House on that.

Mr. KRISHNAMOORTHI. Earlier this month, the President said that he took Vladimir Putin at his word that he did not interfere in Russia, and did not interfere in the 2016 election. Quote, unquote, he said: "Every time he sees me, he says, 'I didn't do that.' And I believe—I really believe that when he tells me that, he means it," quote, unquote.

Mr. Krebs, just a few minutes ago you couldn't point to any reason or dispute, you have no reason to believe that the NSA's conclusions with regard to Russian hacking were inaccurate or incorrect. You defer to the NSA's conclusions. Are you saying that the President is somehow wrong to take Putin at his word, as opposed to deferring to the NSA's conclusions on this topic?

Mr. KREBS. I'd like to clarify one thing real quick.

I have said all along that I agree with the intelligence community's assessment that the Russians attempted to interfere with our election.

Mr. KRISHNAMOORTHI. Good.

Mr. KREBS. What you spoke about earlier was some report attributed to the NSA about a specific State. That is what I defer to the NSA on. I am unable to comment on that. That is not within my agreement. I am focused on information sharing, technical assistance and support to the State and locals. We are in a support role.

Now, to your other comment——

Mr. KRISHNAMOORTHI. Well, let me reclaim some of my time here. You answered the question correctly, in my view, which is that you agree that the Russians did interfere in our 2016 election, or you at least agree with the intelligence community, which knows what it's talking about, that the Russians did interfere in our 2016 election. So are you saying that the President is wrong to disagree with that conclusion, and instead, take the word of Vladimir Putin that Russia did not interfere in our elections?

Mr. KREBS. No, sir. I said I agree with the assessment of the intelligence community on what happened in 2016.

Mr. KRISHNAMOORTHI. Okay. Do you agree with the President that in his assessment, that Vladimir Putin did not actually interfere in our election?

Mr. KREBS. Sir, I was not privy to that conversation. I—look, I'm focused on helping State and local governments for next year.

Every one of us recognize that there is a threat, whether it's from Russia, China, North Korea, or Iran.

Mr. KRISHNAMOORTHI. You're not answering the question, sir.

Mr. KREBS. Yes, sir.

Mr. KRISHNAMOORTHI. You don't have to be privy to that question. You don't have to be privy to that conversation to be able to answer the question. Do you agree with his assessment that Russia did not interfere in our elections?

Mr. KREBS. Sir, I—again, I'll point back to last year's intelligence assessment.

Mr. KRISHNAMOORTHI. Okay. I'll take that as a nonanswer.

Mr. HURD. The chair notes the presence of our colleague, the gentlewoman from Hawaii, Ms. Gabbard, and I ask unanimous consent Ms. Gabbard be allowed to fully participate in today's hearing.

Without objection, so ordered.

Now it's a pleasure to recognize my friend, the gentlewoman from the great State of Hawaii, for 5 minutes for questions.

Ms. GABBARD. I thank the chairman and Ranking Member Kelly for holding this important hearing, and for all of the witnesses for taking the time and coming and sharing your experiences and expertise here. I apologize for missing the first part of the hearing, but I'm sure a number of these topics have been discussed. But I think they all boil down to the immediate task at hand, which is seeing what actions can and should be taken to make sure that our elections are protected.

For our democracy to work, the American people need to have faith and trust in our elections infrastructure that the vote that they cast will actually be counted. And this is why making sure that our elections infrastructure is impenetrable is essential. And that's the task before us here in Congress and before our elections officials.

Mr. Cortes, I'd love to hear your insights regarding Virginia's decision to switch from direct recording electronic voting machines to paper ballots. What were any obstacles that you found in implementing that change? And did you see voter confidence rise once that change was made?

Mr. CORTES. Congresswoman, in terms of our switch over to paper, I think the biggest obstacle that we faced was timing and the proximity to the election. We have statewide elections in Virginia every year. And so we always have very little time to implement changes. I think in this particular round of decertification, subsequent to the DEFCON reporting that came out, you know, the biggest challenges we faced were getting equipment to our State IT agency for them to test and provide us with their assessment.

When it came down to the final decision about what to do with the equipment, our biggest consideration was if we had an issue— if there was some issue reported on election day, would we have the confidence to go out and tell our voters that the results from the machines were accurate, that we can confirm that? And I think ultimately, we determined, in consultation with our wonderful staff at the State IT agency, in their assessment, that we wouldn't be in a position to do that with the equipment we were using.

Without that independent verification, the paper ballot, there would be no way for us to do that. And So I think that ultimately was the moment where, you know, decertification moved forward, and we decided to have paper ballots statewide for this past November.

Our local election officials had less than 60 days before the election, frankly less than 2 weeks before the start of absentee voting, to deploy new equipment. They did a phenomenal job using the exceptionally limited resources that they have and working with—not only in partnership with us, but also in terms of the voting system vendors to get equipment deployed, get ballots printed, do training, do voter education, all within that window. They pulled it off successfully. And so it—you know, I give a lot of credit to our local election officials across the State for being able to do that.

Ms. GABBARD. Thank you.

Ms. Hennessey, I just came in here the last part of your previous statement about making sure that—I think you used the word "impossible," making it so that our elections infrastructure is impossible to hack. Noting the DEFCON report that came out and the fact that it states by the end of DEFCON conference, every paperless electronic voting machine was effectively breached in some manner. Would the implementation of voting machines across the country with some form of an auditable paper record create that impossibility?

Ms. HENNESSEY. So to clarify, I was referring to impossible to hack as a goal of sort of the deterrence by denial model. I don't know that that's achievable, although we shouldn't make perfect the enemy of the good. There's vast improvements that can be made.

Certainly, we should want to move to a place in which systems are both auditable and also audited. And so not just to think about how do we ensure that, a built-in resiliency model. So in the event that there is some form of compromise, some reason to doubt the outcome, that we actually have the system in place to verify it and restore——

Ms. GABBARD. A backup.

Ms. HENNESSEY. Right. And then also, that we actually periodically undertake those checks, right? An auditable system is effectively meaningless if we actually don't undertake the audit.

Ms. GABBARD. This is such an important point. And I think, Mr. Cortes, your testimony is critical to this in answering that question of how do we ensure, with confidence, that you can answer your voters, saying that the election results are accurate. I'm working on legislation that will essentially ensure that whatever the systems the States choose to use in their elections—obviously, that is the freedom of the States to do that—that there be some form of backup in place, a paper, voter-verified backup to ensure exactly that question, and that we can all answer with confidence to voters that the election results are as a result of the votes that they cast.

So I thank you all for being here today.

Thank you, Mr. Chairman.

RPTR FORADORI

EDTR ZAMORA

[4:00 p.m.]

Mr. HURD. I'm going to now recognize myself for some time.

First off, Dr. Blaze, correct me if I'm wrong. I think we may have set a record here today for the number of times DEFCON has been said in a positive way. So all my hacker buddies are going to be happy about that.

In Dr. Blaze and Ms. Hennessey's statements, they've talked about what I would characterize as old school ballot stuffing is one threat. But what a nation-state actor or an intelligence service would try to do, discredit an election, is another threat.

And, Mr. Schedler, Secretary Schedler, the first question to you as the Secretary of State for Louisiana, it's hard to manipulate the votes in an election in your State. Is that correct?

Mr. SCHEDLER. I would say so.

Mr. HURD. Commissioner Cortes, would you agree—not for Louisiana, but for Virginia.

Mr. CORTES. Yes, Mr. Chairman.

Mr. HURD. And, Dr. Blaze and Ms. Hennessey, is it still hard to stuff the ballot electronically in many of these States?

Mr. BLAZE. I think it's very difficult. I think the difficulty that we have is that it's very difficult to prove that it hasn't happened.

Mr. HURD. Well, sure. Sure. It's a trust issue. But when it comes to physically, because of the decentralization, because many of the vote tabulation machines are not connected to the internet, are not connected to one another because of the physical security precautions that are taken around the physical machines that Secretary Schedler talked about at the front, and many of the best practices that Mr. Krebs and his organization has promoted, it makes it hard, right. But the use case that I'm worried about is the credibility of our elections, and not being able to prove something is one of those things.

And for our two secretaries of state, would you agree that the undermining of trust in our voting—in our elections is a bad thing and something we should try to fight against, Mr. Schedler?

Mr. SCHEDLER. I would absolutely agree. I alluded to that in one of my——

Mr. HURD. Microphone, please, sir.

Mr. SCHEDLER. In all due respect, I mean, what has happened, and I think any secretary of state that would address you in all honesty is, is since the last Presidential election and all the rhetoric and all the committee reports and all the things that are going around this, if you don't think that has had a tremendously negative feeling to voters, we see it.

I just got out of an election for the mayor of New Orleans, an open seat, that had a 32 percent voter turnout in Orleans Parish, and we had a statewide election special for State treasurer. When I look at the statewide overall voter turnout, 12–1/2 percent. That is absurd in this country.

And I'm not going to sit here—one of my most frequently asked question is, Why, Secretary Schedler? And I could give you a litany of 10 or 15 things. One of them I know you all wouldn't want to hear.

But, for certain, the rhetoric that has gone around from this past election has tremendously deterred voter confidence. And it's a balancing act for a guy like me and Mr. Cortes because we're up here trying to defend the integrity of a system——

Mr. HURD. For sure.

Mr. SCHEDLER. —and yet it's being torn down as I speak.

Mr. HURD. Right. And that's one of the reasons to have this hearing——

Mr. SCHEDLER. Yes, I'm respectful of that.

Mr. HURD. —is to get smart folks in a dispassionate way talking about the realities. And then how can we identify certain things that we can do together in a way to ensure that that trust is there so that we get more than 12 percent?

Now, I would also say that I was at a panel in South by Southwest with a bunch of YouTube stars, and I didn't know any of the YouTube stars, but when you added all their fans together, it was almost a billion. And the woman, Ms. Lardy, who does digital stuff with a rock, said, if a movie performs poorly at the box office, do you blame movie goers or do you blame the movie? And I think in this case, a lot of times we want to blame voters when we're not providing the voters something for them to come out and purchase by pulling a lever. So that is an aside.

Mr. Cortes, was there any funny business in your elections in Virginia a couple of weeks ago?

Mr. CORTES. Mr. Chairman, I think we had a——

Mr. HURD. That's a technical term too, by the way, "funny business."

Mr. CORTES. I believe we had a very successful election in Virginia a couple weeks ago. We actually—I'm sorry to hear that you all had a lower turnout in your statewide. We had record turnout in our statewide race for Governor, Lieutenant Governor, Attorney General, as well as our House of Delegates, and it was a very successful—we did not receive any complaints related to voting equipment, which was a first in the time that I've been there. We had a very successful day across the Commonwealth. Very few issues. You know, you always get the occasional place where they have delivered equipment to the wrong place and they may open a couple minutes late, but we had no major systemic issues that took place.

Mr. HURD. Well, touche to Virginia.

And, Mr. Krebs, some specific questions here. How many cyber hygiene services over the internet—for internet-facing systems can your organization do in a calendar year? And I realize that's a—you know, you can round number—you can ballpark it for us.

Mr. KREBS. That's tough because, frankly, engineeringwise, it's—I don't want to say infinity, but it's—frankly, it's very, very scalable.

Mr. HURD. So you're not concerned about the over 10,000 voting jurisdictions requesting that particular service that you feel like you'll be able to meet the need——

Mr. KREBS. No, sir, I think the challenge there would be intake, would be signing up on the legal agreement side, figuring out the IP ranges and deploying.

Mr. HURD. Good copy. How many risk and vulnerability assessments can you do in a calendar year?

Mr. KREBS. That is a different question. Risk and vulnerability assessments are time and manpower limited. In terms of the number on a given year, it'd be—let me put it this way: To do one risk vulnerability assessment it takes 2 weeks.

Mr. HURD. Two weeks.

Mr. KREBS. It's a week onsite and a week report drafting. What we're doing in the meantime, though——

Mr. HURD. And you have about 130 people that are able to do this function?

Mr. KREBS. I'd have to get back to you on the specific numbers on the Hurd teams, but it's—you know, we are manpower limited there, but what we—and the reason for that, and you just made my job a little bit harder with the NGT Act, but this all comes out of the same pile of assessments as Federal IT, the high-value asset. And so if we're going to do some modernization activities, congratulations, but that's going to make my job a little bit tougher. That also is the critical infrastructure community. So it's all in one——

What the critical infrastructure designation did for the election subsector is allowed me to reprioritize. So now I'm able to put any requests up at the top of the list. We just completed an RVA last week. I reviewed the product earlier this week, and it is an impressive document. I'd like to do more. We are going to continue to prioritize, upon request, these are voluntary products, but keeping in mind that a number of States have their own resources or private sector resources. So, you know, we're not looking to serve for every single State, but we are looking to reprioritize to address.

Mr. HURD. And this next question is for Secretary Schedler, Commissioner Cortes, and Mr. Krebs, and maybe Secretary Schedler, you take the first swing at this. And this is probably better—you know, this question I'm asking you of this as your former hat at NASS. And what role exactly does NIST and the HAVA Standards Board play? And maybe if—Mr. Krebs, if you're more appropriate to answer that question, you know, I'll leave it up to you all.

Mr. SCHEDLER. I mean, it certainly assists us in certification issues and some of those outlier issues that we have. But, I mean, I think it's more of a collective whole, NASS, whether it be with the Election Commission, NIST, or any of us, I mean, we collaboratively all work together. We share information through our executive director, Ms. Reynolds, here in Washington.

So, I mean, I think it's a good thing. I wouldn't want to necessarily disband that, but I think it's more looking at it as a collective whole and our new partners in Homeland Security. I mean, I alluded that we were very much against critical infrastructure. We're in it. We're in a cooperative spirit. We're trying to get our security clearances done at this time and we're going to continue that.

Mr. HURD. So, Secretary, am I hearing DHS is not trying to take over?

Mr. SCHEDLER. No, sir, I don't think so. Not yet. I'll give you a call.

Mr. HURD. Please do. Please do. And are folks comfortable with the security clearance process? I know we're trying to get every secretary of state and I believe two additional——

Mr. SCHEDLER. Yes.

Mr. HURD. —folks. And your indication is that folks are happy with that process and how it's done?

Mr. SCHEDLER. Yes, sir, we are. That's the first good step that we can share some information.

Mr. HURD. Commissioner Cortes, do you have, you know, any information to disagree with that or——

Mr. CORTES. Mr. Chairman, I think, you know, from our perspective in Virginia, having had a statewide election, we had an opportunity to work very closely with DHS throughout the year in preparation for that and really figuring out how to leverage the Federal resource offerings, along with what our State IT agency provides, as well as the Virginia National Guard. So we've worked very collaboratively with them. I think the creation of the coordinating council I think will be exceptionally helpful going forward.

I think when it comes to the EAC and NIST, EAC's role in this has been—you know, hasn't been as highlighted as I think it should be. I think they've been really critical in opening up that dialogue between DHS and the elections community, as well as facilitating a lot of the meetings and interactions that have taken place. So they've been exceptionally helpful there.

When it comes to NIST, I think for us, and I think going forward, you know, what we need to look at is the—you know, the NIST cybersecurity framework is something that our State IT standards are premised on and that we utilize for our voting equipment, security, and our electronic pollbook security. So those standards being there are very helpful to us and provide the level of expertise and, you know, things to look for and test against that we would not, you know, with our State resources be able to recreate on our own. So everybody's been exceptionally helpful.

Mr. HURD. That is very helpful feedback.

And, Mr. Krebs, kudos to you for your leadership in that process.

And maybe to anybody at this panel, why does EAC have $300 million in unspent funds? Does anybody have any unknown—none of you all sit at EAC? Would anybody like to offer a question?

Mr. SCHEDLER. They must have some of those HAVA dollars that we need.

Mr. HURD. And that's what we're trying to get at is, is there an opportunity there to reprogram some of those funds to help some of the municipalities that need to upgrade some of their systems?

Mr. SCHEDLER. Yes. And that was a tongue-in-cheek comment, because I'm on the advisory—I truly don't know——

Mr. HURD. Can you hit the button?

Mr. SCHEDLER. I truly do not know what that balance is, and, I mean, I just—it's certainly something to look at. I think we got to look at any and all avenues of funding because we do need assistance in the State, I can assure you. Just like Federal Government, States are in budgetary issues. I know certainly Louisiana is. And at this critical point of trying to replace equipment because of some of the subject matter we're talking about here, you know, we're scrambling to try to find a way to do that, and I'm getting ready to go out on an RFP, so——

Mr. HURD. Mr. Krebs, any comments?

Mr. KREBS. I think what we're talking about now, and I do wish that Matt Masterson, the chairman of the EAC, was here. I met with his yesterday. I think he's in Iowa right now doing some training.

EAC has been a critical partner. When DHS got into this game—it was before my time—but when we got into this game last year, it was kind of a brave new world, didn't have a relationship. EAC was critical in bridging the gap and developing relationships with Louisiana, Virginia, and the rest of the States.

NIST is also a partner. I think Dr. Blaze would agree that NIST is probably reputationally unmatched in terms of cybersecurity and cryptography excellence. And they are a critical partner in standards development going forward.

And then on the information sharing piece—one last thing. I do want to touch on the classified and the clearances piece. Clearances, as has been pointed out, clearances and the sharing of classified information is important, but we are, in the meantime, focusing on that declassification effort. It is critically important that we speed up that process to get it out, tear lines, all that good stuff. But in the meantime, when something truly sensitive comes in and someone doesn't have the clearance but needs to see a piece of information, I personally have the capability to authorize one-day read-ins.

So we have a suite of services and tools and capabilities that we can—to make sure that our partners have the information they need.

Mr. HURD. Well, Mr. Krebs, that's why DHS is the bellybutton for information sharing with municipalities and the private sector, because I believe you're the only organization that can truly achieve need to share versus need to know, and continuing down that line is important.

Dr. Blaze, when it comes to the kinds of systems, the actual vote tabulation machines, and you've talked a lot about the scan, you know, version, one of the concerns I have about some of the legislation that's being discussed is talking specifically about a type of machine versus an outcome. And is it fair to say that, based on your research and your activity, that you're saying there needs to be an artifact that can be checked in the case that a system is suspected of compromise?

Mr. BLAZE. That's correct. The two important properties are, first, that there be a paper artifact of the voter. Optical scan paper is an example of a system that does that. That's probably the best state-of-the-art technology that we have right now. The second property is that we have a mechanism for detecting compromise of the software that tabulates votes, and that's the risk limiting audit feature.

Put together, those achieve or approach what we call strong software independence, which means that, even if the software is compromised, we still can learn the true outcome of the election.

Mr. HURD. Good copy.

Ms. Hennessey, do you have anything to add to that or disagree with?

Ms. HENNESSEY. No, I would agree with everything Dr. Blaze said.

Mr. HURD. Thank you.

And my last question—and, Chairman Palmer and Ranking Member Kelly, thanks for the indulgence—is slightly outside of the bounds of the hearing topic today. But as we talk about the importance of protecting our voting systems and trying to fight this effort to erode trust in our national institutions, disinformation is the tool that hostile intelligence services are going to continue to use against us.

And I would just welcome, and really, Secretary Schedler and Commissioner Cortes, what is the role of States in helping to combat disinformation, specifically when it comes around election time?

And, Dr. Blaze and Ms. Hennessey, I'd welcome your thoughts.

And then, Mr. Krebs, I'm going to give you 30 seconds to say whatever you want to say.

Secretary Schedler.

Mr. SCHEDLER. Well, I mean, it's the old fashioned way. You get out there and you communicate with people and you get on the airwaves on radio and you get on TV and you get in the newspaper and you combat some of this. Because, I'll be honest with you, I had an individual just this morning that called me—or, excuse me, text me from the previous election, and he was convinced that our machines were connected to the school internet system, because I guess it was plugged into a plug. I don't know, but, I mean, it's those types of things in every real day of a secretary of state or an election official across the country that we combat. It's just part of the job. I will tell you, it has become on steroids in the last 24 months.

Mr. HURD. As a Member of Congress, I would say I understand those concerns. Thank you, sir.

Commissioner Cortes.

Mr. CORTES. Mr. Chairman, I think it's really about being open and transparent in the process and having, you know, processes in place and working as election officials to make sure voters are comfortable with the process and getting out there and combating any misinformation about how the process works. And I think our focus on transparency and doing things like post-election audits, having equipment that had some sort of verifiable backup, these are all things that we can do to provide voters assurance that they can actually see and observe and not just tell them everything's okay.

We're I think at a stage with our election processes where people need to be able to understand what steps we're taking and how we're doing, you know, to make sure that things are okay, to make sure that their voting experience is a good one, and that their votes are counted accurately.

Mr. HURD. Good copy.

Dr. Blaze.

Mr. BLAZE. So I think the most important thing, from a technology perspective, is that the voting technology allow us to refute those who say that the election was tampered with. And, unfortunately, many of the systems in use today, even if they haven't been tampered with, aren't designed in a way that allows us to do that.

So I look forward to seeing a shift toward technologies that are more robust and that allow us to do meaningful recounts.

Mr. HURD. Ms. Hennessey.

Ms. HENNESSEY. To bolster credible institutions now, and so to not—to sort of resist any temptations of partisanship so that in the event—so that there are those enduring credible voices. And the closer we get to elections, the actual election date, the higher the risk of politicization sort of infecting that process comes, which increases the importance of setting neutral standards now, both for the types of information that will be shared and also for response options.

Mr. HURD. Thank you.

Final words, Mr. Krebs?

Mr. KREBS. Yes, sir. I think my four co-panelists have said it quite well. A key tenet of countering information operations is shining a light on the activity. So what we have ahead of us, and we were just talking about it before the hearing today, is, we have some coordination work. We need to do some incident response planning, develop a playbook, so if something pops up on social media, Twitter, or whatever it is, we get the call, we can work to refute the information, and we can push it out through a clear trusted channel to the American people so they can retain confidence in our election systems.

Mr. HURD. Well, I want to thank all of you all for helping to shine a light on the activities that our States and the Federal Government is doing to ensure that the American people can have the trust in their elections. That's what makes this country great, is when we're faced with adversity, we all do pull together. And I appreciate you all appearing before us today and the flexibility in your travel schedules.

The hearing record will remain open for 2 weeks for any member to submit a written opening statement or questions for the record.

If there's no further business, without objection, the subcommittees stand adjourned.

[Whereupon, at 4:20 p.m., the subcommittees adjourned.]

APPENDIX

Material Submitted for the Hearing Record

Cybersecurity of Voting Machines
House Committee on Oversight and Government Reform
Subcommittees on Information Technology and Intergovernmental Affairs
2:00 PM, Wednesday November 29, 2017
2154 RHOB
Rep. Gerald E. Connolly (D-VA)

Thank you, Mr. Chairman for holding this important hearing to examine the cybersecurity of voting machines. The right to vote is one of the most sacred and fundamental rights of United States citizens. Voters have every right to believe that when they go to the polls to cast their vote, that it will count, and count correctly.

However, after last year's Presidential election, questions have been raised about foreign influence in our election system. On January 6, 2017, the U.S. Intelligence Community released an unclassified report detailing an unprecedented, deliberate, and multi-faceted campaign by Russia to interfere in the 2016 U.S. presidential election. The USIC assessed that Putin directed this interference not only to "undermine public faith in the U.S. democratic process," but also "to help President-elect Trump's election chances when possible by discrediting Secretary Clinton and publicly contrasting her unfavorably to him." That should trouble every American. One of our most cherished institutions, democratic elections free of foreign interference, was attacked. Congress must come together in a bipartisan fashion to demonstrate that there is a cost to such attacks on American democratic institutions. This is about country not party.

Last month, the Subcommittee on Information Technology held a hearing to examine whether federal laws and regulations are adequate to prevent foreign actors from influencing our elections through digital advertisements and sham social media accounts. Today, we will examine potential cyber threats facing voting machines and what can be done to secure election systems against possible cyber attacks. On September 27, 2017, the Department of Homeland Security (DHS) notified 21 states, including the Commonwealth of Virginia, that Russian government hackers tried to breach their systems during the 2016 elections. This occurred three weeks after Virginia's election supervisors directed counties to ditch touchscreen voting machines before this year's elections, saying the devices posed unacceptable risks. According to a September 22, 2017 article in *The Washington Post*, during the 2016 elections, hackers were already able to penetrate computer systems in a handful of states in order to tamper with voter registration files. And while there is no current evidence that hackers tampered with any voting machines, I believe there will be efforts to do so in 2018 and beyond.

Most alarmingly, hackers gathered at a conference in Las Vegas this past summer and quickly hacked into voting machines that have been used by several states, including one that was used by Virginia through 2015. It took less than a day for attendees at the conference to find and exploit vulnerabilities in five different types of voting machines. These hackers quickly found what state actors who seek to influence our elections will discover eventually, if they haven't yet: that voting machines are inadequately secured and the software they use are often not up to modern standards. Hackers were able to break into voting machines through Wi-Fi and upload malware to them. Hackers also noted that voting machines often contained significant lapses in physical security such as exposed USB ports that would allow for someone seeking to crash the system to upload malware to the machine.

To address the vulnerabilities of voting machines, states and local officials must focus on cybersecurity year-round, not just in the months and weeks leading up to an election. There is also critical need for states to replace their aging voting equipment with new, auditable systems, such as optical scanners and paper ballots. In last year's election, 42 states used voting machines that are more than a decade old. These machines are especially vulnerable to modern hacking techniques because they rely on unsupported operating systems and software that no longer receive regular security updates.

However, purchasing new voting machines or upgrading existing ones are not cheap. Some estimates put the cost of a nationwide modernization program at $500-$600 million. As many states face tightening budgets, they would be hard pressed to spend millions of dollars to upgrade machines that are used, at most, a few days per year. That is why it is disappointing that the House Administration Committee voted earlier this year to eliminate the Election Assistance Commission (EAC), a federal agency established by Congress to help states improve their voting systems in the aftermath of the disputed 2000 presidential election. Support for this agency is more important than ever following unprecedented foreign interference in the 2016 presidential election, widespread voter suppression efforts, and false accusations of massive voter fraud.

Instead eliminating the EAC, I introduced the Fair, Accurate, Secure, and Timely Voting Act, (FAST Voting Act) (H.R. 1398) that would strengthen the Commission's ability to assist states who are seeking to improve their voting systems and tackle real issues states and localities face in conducting elections. The legislation is a competitive grant program that would enhance voting system security, improve voter participation, and encourage automatic voter registration. The bill is modeled after the Race to the Top education initiative and authorizes the EAC to award grants to states that are striving to improve access to the ballot, establish automatic voter registration, or implement additional election security measures or innovations.

At the federal level, the Department of Homeland Security (DHS) must work with states to share cyber threat information and help states respond to those threats in real time. The Election Infrastructure Coordinating Council recently convened by DHS will allow the Department to share threat information, advance risk management efforts, and offer cybersecurity services available to state and local partners. These services include comprehensive threat assessments, cyber hygiene scans, penetration testing, and advising on protecting physical assets. These services can be particularly valuable to local election officials who often do not keep information technology and cybersecurity experts on staff.

Protecting the integrity of our democracy is not a partisan issue. We must work together to ensure that all eligible voters are able to vote securely, efficiently, and without a doubt in their mind that their vote will be counted.

TREY GOWDY, SOUTH CAROLINA
CHAIRMAN

ONE HUNDRED FIFTEENTH CONGRESS

ELIJAH E. CUMMINGS, MARYLAND
RANKING MINORITY MEMBER

Congress of the United States

House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
2157 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6143

MAJORITY (202) 225-5074
MINORITY (202) 225-5051
http://oversight.house.gov

October 20, 2017

The Honorable Robert Kolasky
Acting Deputy Under Secretary
National Protections and Programs Directorate
Department of Homeland Security
Washington, DC 20528

Dear Acting Deputy Under Secretary Kolasky:

Last month, the Department of Homeland Security reportedly notified election officials in 21 states that Russian government hackers had targeted those states during the 2016 election.[1] We are writing to request copies of these notifications and additional documents, as well as a briefing from top Department officials on these matters.

The Department's notifications to these states came nearly a year after the election and three months after the Department publicly disclosed that individuals connected with the Russian government sought to hack voter registration files and public election sites in 21 states.[2] They also came after numerous other reports that Russia engaged in a multifaceted campaign to disrupt the 2016 election, including widespread cyber-attacks on state-election infrastructure systems.[3]

The Department's recent convening of the Government Coordinating Council for the Election Infrastructure Subsector, with representatives from the Election Assistance Commission, the National Association of Secretaries of State and state and local election officials, will hopefully facilitate the sharing of information and expertise.[4]

[1] *DHS Tells States About Russian Hacking During 2016 Election,* Washington Post (Sept. 22, 2017) (online at www.washingtonpost.com/world/national-security/dhs-tells-states-about-russian-hacking-during-2016-election/2017/09/22/fd263a2c-9fe2-11e7-8ea1-ed975285475e_story.html?utm_term=.55b916d66ca3).

[2] *Russians Tried to Hack Election Systems in 21 States, U.S. Officials Say,* Chicago Tribune (June 21, 2017) (online at www.chicagotribune.com/news/nationworld/ct-homeland-security-chief-intelligence-panel-20170621-story.html).

[3] *See, e.g.,* Department of Homeland Security, *Joint Analysis Report: GRIZZLEY STEPPE—Russian Malicious Cyber Activity* (Dec. 29, 2016) (online at www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf); Office of the Director of National Intelligence, *Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution* (Jan. 6, 2017) (online at www.dni.gov/files/documents/ICA_2017_01.pdf).

[4] Department of Homeland Security, *DHS and Partners Convene First Election Infrastructure Coordinating Council* (Oct. 14, 2017) (online at www.dhs.gov/news/2017/10/14/dhs-and-partners-convene-first-election-infrastructure-coordinating-council).

We request that you produce, by October 31, 2017, copies of the notifications sent by the Department to these 21 states, as well as all accompanying materials relating to Russian government-backed attempts to hack state election systems.

We also request a briefing from appropriate Department officials within the same timeframe on the following issues:

(1) the types of voting equipment that were attacked;
(2) the timeline by which the Department provided information to these states and the reasons for not sharing additional information sooner;
(3) services and trainings offered to states to detect and prevent cyber-attacks;
(4) plans to work with states to detect and prevent future cyber-attacks; and
(5) the operational plans and goals of the newly convened Election Infrastructure Coordinating Council.

If you have any questions, please contact Jennifer Daehn with the Democratic Committee staff at (202) 225-5051. Thank you for your consideration of this request.

Sincerely,

Elijah E. Cummings

Elijah E. Cummings
Ranking Member
Committee on Oversight and
Government Reform

Robin L Kelly

Robin Kelly
Ranking Member
Subcommittee on
Information Technology

cc: The Honorable Trey Gowdy, Chairman
Committee on Oversight and Government Reform

The Honorable Will Hurd, Chairman
Subcommittee on Information Technology

Detroit's election woes: 782 more votes than voters

Another 382 Detroiters were listed as voting but their ballots never showed up in the count.

John Wisely and JC Reindl, Detroit Free Press

December 18, 2016

Whether the result of machine malfunction, human error or even fraud, the unexplained voting discrepancies in Detroit last month were not sizable enough to affect the outcome in Michigan of the presidential election, according to a new Free Press analysis of voting precinct records.

In 248 precincts, there were a total of 782 more votes tabulated by voting machines than the number of voters listed as picking up ballots in the precincts' poll books. That makes up just three-tenths of 1% of the total 248,211 votes that were logged in Detroit for the presidential election. That number was far too small to swing the statewide election results, even in this year's especially tight race that saw a Republican win Michigan for the first time since George Bush in 1988.

Donald Trump carried Michigan by 10,704 votes, or 47.5% to 47.3%, according to the final results submitted to the Michigan Secretary of State. But in Detroit, Democrat Hillary Clinton trounced Trump, winning 95% of the vote to his 3%.

The Free Press analysis found there were 248 precincts in Detroit where voting machines tabulated more Election Day votes than people who were counted as checking in to vote. The affected precincts represent 37% of the city's 662 precincts.

Most of those overages were by small amounts — on average about 3 votes — with the largest being 12 votes in a single precinct. Those small numbers, which add up to 782 total spread out across more than 200 precincts, tend to point to human or machine malfunction as the culprit, rather than widespread fraud.

In 158 precincts, the number of ballots tabulated by the optical-scanning voting machines was inexplicably less than the number of people who signed in to vote. At least 362 ballots were not counted in those precincts, even though the voters had been listed in poll books.

Altogether, the total of over-counted and under-counted ballots was about 1,144. As a result, nearly 60% of Detroit's precincts weren't eligible for recount because the number of ballots in the ballot box didn't match the number of people listed as voting in the poll book.

The Free Press analysis came from handwritten tabulations logged by the Wayne County Board of Canvassers. The numbers are approximated because notes in eight precincts were illegible or unclear. This is the first time that actual figures for over-counted and under-counted votes have been reported

Detroit's inability to reconcile its ballots with its voter lists was exposed in the recount requested by Green Party presidential candidate Jill Stein that was later ordered stopped by the Michigan Supreme Court. The discrepancy became national news, including headlines suggesting voter fraud.

Reasons for the under-counted and over-counted votes are unclear, although in some cases people may have signed in to vote, then left before casting their ballots because of long lines. Machine malfunctions also may have played a role; on Election Day, more than 80 optical vote scanners broke down in Detroit.

Detroit City Clerk Janice Winfrey and Elections Director Daniel Baxter could not be reached for comment Sunday regarding these latest findings. Winfrey told the Free Press last week that the city's decade-old voting machines broke down and caused problems throughout Election Day and that the city has struggled for years to recruit younger people to work the polls. Most Detroit poll workers are retirees with an average age of 68 and they typically work 15-18 hours on Election Day for a $150 paycheck.

Winfrey said Detroit will be getting new voting machines in time for the 2017 mayoral and City Council elections.

Under Michigan law, precincts cannot be recounted when the number of voters in the poll book doesn't match the number of ballots in the ballot box. Almost 60% of Detroit's precincts were mismatched — either having too many or not enough ballots to match poll books — and ineligible for recount, according to the Wayne County Clerk's Office.

Detroit wasn't the only place in Michigan with recount problems. There was at least one ineligible precinct in each of the 22 counties where the recount had gotten under way before being halted by the court, according to Michigan Secretary of State records.

The state Bureau of Elections plans to conduct audits of about 20 Detroit precincts that couldn't be recounted. Those ballots are to be brought to Lansing for an audit that should last for at least three weeks, said Chris Thomas, director of elections for the state. "We don't have any suspicion of fraud. We generally approach this as human error," Thomas said last week. "We're going to take a look at them to make sure there's not a need for further explanations."

Bill Ballenger, longtime Michigan political analyst and founder of the Ballenger Report, said Sunday that even though the number of questionable votes in Detroit was apparently too small to affect this election, the discrepancies are still disconcerting because the race was so close and they demonstrate the need for an audit.

"If there's one thing good that came out of the recount petition by Jill Stein, it's that it revealed there are some problems," he said.

Ballenger noted how the outcome of the 2000 presidential election between George W. Bush and Al Gore hinged on just 537 votes in the state of Florida. That is fewer than the number of questionable Detroit votes.

"If this election had turned out to be as close as Florida in 2000, this would be a huge story right now," he said.

#

Question#:	1
Topic:	Russian hacking
Hearing:	Cybersecurity of Voting Machines
Primary:	The Honorable Val Demings
Committee:	OVERSIGHT & GOV RFORM (HOUSE)

Question: At the hearing, Rep. Kelly introduced into the record a letter she sent on October 20, 2017, with Ranking Member Elijah Cummings. The letter requested "copies of the notifications" the Department of Homeland Security (DHS) provided to 21 states reportedly targeted by Russian hacking efforts. The letter also requested copies of all documents "related to the Russian government-backed attempts to hack state election systems." Attached is a copy of the letter that Rep. Kelly introduced into the record.

According to press reports, the following states received notifications from DHS that they were identified as targets: Washington, Oregon, California, Colorado, Illinois, Alaska, Arizona, Oklahoma, Texas, North Dakota, Minnesota Wisconsin, Iowa, Ohio, Alabama, Florida, Pennsylvania, Virginia, Maryland, Connecticut, and Delaware.

On the day before the hearing, DHS produced only an email with a short script that DHS employees apparently read over the phone to state election officials. It is only 13 sentences long and does not refer to any specific state or attack. Rather, it is a generic script that provides no specific information.

DHS has yet to produce any of the other requested documents.

Please immediately produce copies of all documents related to the Russian government-backed attempts to monitor, penetrate, or hack state election systems during the presidential election campaign of 2016, including but not limited to the tools the attackers used, the tactics they utilized, the results of your conversations with these states, and the steps you took to follow-up.

Response: The Department will work with the Committee to provide additional information, as appropriate. In 2016, DHS alerted chief state election officials of relevant cybersecurity threats. DHS issued several public statements between August and Election Day to share information regarding the threat and urged election officials to seek cybersecurity assistance from either DHS or other experts. The former Secretary held multiple phone calls with election officials to highlight the seriousness of the threat. DHS and the Office of the Director of National Intelligence declassified attribution and alerted the public to malicious activity directed towards our elections on October 7, 2016. Several days later, DHS's National Cybersecurity and Communications Integration Center (NCCIC) and the Federal Bureau of Investigation (FBI) published and shared with election officials a joint analysis report containing recommendations and over 650 technical indicators of compromise to assist election officials with detecting

Question#:	1
Topic:	Russian hacking
Hearing:	Cybersecurity of Voting Machines
Primary:	The Honorable Val Demings
Committee:	OVERSIGHT & GOV RFORM (HOUSE)

malicious activity on their networks. Some of these indicators had previously been classified and were pulled from analysis of previous incidents relevant to the threat. Between August and Election Day, DHS and other interagency partners shared several other products, including best practices specific to election infrastructure, intelligence assessments, risk assessments, and technical information to assist election officials with network protection. DHS provided some of these documents to House Oversight and Government Reform Committee Staff on September 16, 2016 and September 26, 2016.

Question: For each of the 21 states, please provide details of your notification to state officials of the attempted cyberattacks, including:

the date of the notification;
the names of the state officials or offices that were notified;
the name of the DHS division that provided the notification;
whether it was a telephonic notification, or by other means;
services offered during the notification; and
the dates of any subsequent communications relating to cyberattacks with state officials.

Response: During the 2016 election period, DHS and its partners shared information—specifically information regarding targeting of voter registration systems in some jurisdictions—with state and local governments to increase awareness of threat activity and enable recipients to check their systems for similar activity. Through intelligence and information sharing efforts, including with other federal entities, trusted third parties like the Multi-State Information Sharing and Analysis Center (MS-ISAC), and state and local cybersecurity officials, the Department and its partners learned of specific communications or attempted communications from malicious information technology infrastructure to known state or local government networks in at least 21 states. At the time these communications were identified and highlighted to network operators, the U.S. Government had not yet concluded assessments of attribution and therefore did not attribute the incidents to Russia.

In some cases, state and local government network operators further shared the identified communications or attempts with election officials, but not in all cases. In more recent discussions with some of these network operators, it is clear that a major reason for not sharing further with elections officials included the fact that the majority of the observed communications were preparatory in nature and indicated no evidence of compromise – low-level activity that generally does not require reporting to senior executives.

Some Secretaries of State and other state chief election officials expressed frustration at not being informed whether their states were included in the 21 states referenced in

Question#:	1
Topic:	Russian hacking
Hearing:	Cybersecurity of Voting Machines
Primary:	The Honorable Val Demings
Committee:	OVERSIGHT & GOV RFORM (HOUSE)

DHS's June 2017 testimony before Congress. To address these concerns, DHS called Secretaries of State and State Election Directors to let them know if their state was or was not included in DHS's assessment. These were not victim notification calls, and there is no new information on the 2016 cyber targeting beyond what was discussed in the June testimony. State officials were, for the most part, already notified of the activity in 2016. We also discuss cybersecurity measures and threats with State and local officials on a daily basis, including within the Government Coordinating Council, the MS-IAC, Cybersecurity Advisors, Protective Security Advisors, and other venues. These interactions are now a common occurrence and regularly apply lessons learned from the 2016 Election, including sharing information and best practices on spear phishing, SQL injection, and other known tactics, techniques, and procedures.

Question: Did DHS notify any other states that their election infrastructure had been targeted by cyberattacks in 2016? If so, please provide similar details of your notifications to those States, using the format above.

Response: No, the 21 states are inclusive of DHS's assessment of the scale and scope of malicious activity.